Sample Draft Security Design Document

Lot II – Systems Integration

Your Application (XYZ)/
123 System (123)
Integration

XYZ Version 1.0
Security Design Document (SDD)

Prepared by:

XYZ Project Office
Your Street Address
Your City, ZIP

dd/mm/yy

Executive Summary

The Security Design Document (SDD) satisfies one of the documentation requirements necessary to meet Class C2 system certification as specified in Department of Defense (DoD) 5200.28-STD; *"Department of Defense Trusted Computer System Evaluation Criteria (TCSEC),"* 26 December 1985.

The purpose of this SDD is to define the Your Application (XYZ) philosophy of protection, identify the security safeguards that comprise the system Trusted Computing Base (TCB), provide a detailed description of each security safeguard, and explain how the security safeguards satisfy the protection objectives and meet the Trusted Computer System Evaluation Criteria (TCSEC) Class C2 security requirements defined in DoD 5200.28-STD. This SDD is a living document that must be updated to incorporate changes in security safeguard design, philosophy of protection, and system security policy objectives.

Source documents used for development of this manual were DoD 5200.28-STD; National Computer Security Center (NCSC)-TG-007, Version-1, *"A Guide to Understanding Design Documentation in Trusted Systems,"* 2 October 1988, and Military Health System (MHS) *"Automated Information System (AIS) Security Policy Manual," April 1996.*

Table of Contents

List of Figures

List of Tables

Introduction

Purpose

The purpose of this Security Design Document (SDD) is to define the Your Application (XYZ) philosophy of protection, identify the security safeguards that comprise the system Trusted Computing Base (TCB), provide a detailed description of each security safeguard, and explain how the security safeguards satisfy the protection objectives and meet the Trusted Computer System Evaluation Criteria (TCSEC) Class C2 security requirements defined in Department of Defense (DoD) 5200.28-STD, *"Department of Defense Trusted Computer System Evaluation Criteria (TCSEC),"* 26 December 1985. This SDD is a living document that must be updated to incorporate changes in security safeguard design, philosophy of protection, and system security policy objectives.

Applicability and Scope

The information in this document provides system managers, developers, and security certification officials with a baseline for measuring security design effectiveness and managing design changes that impact security throughout the XYZ system's lifecycle. This document explains how the XYZ philosophy of protection is translated into technical solutions that make up the system TCB and describes how the system TCB enforces the philosophy of protection. This document also describes the security safeguards associated with XYZ external system interfaces that are considered an integral part of the system TCB. The term TCB refers to all protection mechanisms in an Automated Information System (AIS), including hardware, firmware, and software, all of which are responsible for enforcing security policy.

System Overview

The XYZ Version 1.0 (XYZ 1.0) is a multi-user system employing client server technology. XYZ is composed of various Commercial-Off-The-Shelf (COTS) and commercially developed software applications residing on a Microsoft Windows NT based IBM-compatible client workstation and UNIX based Hewlett-Packard (HP) 9000 Model servers. XYZ system security safeguards are enforced by elements of the HP UNIX operating system, COTS application, and commercially developed software. In addition, XYZ derives complementary controls from the 123 System (123) external interface.

Reference Documents

The following publications contain information pertaining to AISs processing sensitive unclassified information and were followed in developing the XYZ design architecture.

- DoD Directive (DoDD) 5200.28, *"Security Requirements for Automated Information Systems (AISs),"* 21 March 1988.

- DoD 5200.28-STD, *"Department of Defense Standard Trusted Computer System Evaluation Criteria (TCSEC),"* 26 December 1985.

- DoD 5200.2-R, *"Personnel Security Program,"* January 1987.

- DoD 5400.7-R, *"Department of Defense Freedom of Information Act Program,"* June 1987.

- DoD 5400.11-R, *"Department of Defense Privacy Program,"* 6 June 1982.

- DoD Directive 5000.1, *"Defense Acquisition,"* 15 March 1996.

- Office of the Secretary of Defense (OSD)(DA&M) Memorandum, *"Privacy Act Computer Matching Programs,"* 19 July 1989.

- Office of Management and Budget (OMB) Circular No. A-130, *"Management of Federal Information Resources,"* 8 February 1996.

- National Computer Security Center (NCSC)-TG-007, Version-1, *"A Guide to Understanding Design Documentation in Trusted Systems,"* 2 October 1988.

- Military Health System (MHS) *"Automated Information System (AIS) Security Policy Manual," April 1996*

- *XYZ 1.0 Consolidated Technical Specification Document (Draft),* 31 December 1996.

- Freedom of Information Act of 1967 (P.L. 90-23).

- Privacy Act of 1974 (P.L. 93-579).

System Description

System Overview

The XYZ 1.0 application has been designed for DoD Medical Treatment Facilities (MTFs) to serve as a user interface for hospital and clinical information systems, such as 123 System (123). The application helps health care providers retrieve, record and store data, and communicate orders about their patients. The system manages information by coding visits and tracking costs of episodes of care while enhancing the reliability and availability of clinical data. This enables health care providers to have prompt access to the required patient information. In effect, XYZ 1.0 transforms the ambulatory clinical environment by automating most of the documentation tasks.

The XYZ 1.0 software application, supported by a Graphical User Interface (GUI), provides the user with the following functional capabilities:

- This and That;
- More stuff;
- Other functionality;
- Notes;
- Orders, Orders Maintenance; and
- Coding.

Technical Description

The XYZ 1.0 application uses a modified, three-tier client-server architecture consisting of presentation, application, and database layers. This multi-tier approach provides the flexibility to distribute the program’s logic throughout the Visual Basic client, the relational and image database servers, and the clinic servers. It also provides maximum performance by reducing traffic on existing networks, improving data security, and providing improved response time to user requests.

A GUI resides on a desktop Personal Computer (PC) running Windows NT Version 3.51 (or higher) client. Healthcare providers (clinicians, technicians, doctors) retrieve, input, and archive patient data through the GUI by using keyboard, pen stylus/writing tablet, or high-resolution Optical Character Reader (OCR) scanner.

All image files are retrieved from the master image database and cached locally through batch and transaction processes. Text files are retrieved and archived transactionally from the relational database.

An interface application, Hobbit, receives appointment information, patient data, and static table data from the 123 system and inputs it into the XYZ 1.0 relational database. The XXX System (XXX) interface downloads appointment, coding, and disposition data for completed and cancelled appointments from the relational database each night.

XYZ Hardware

System Servers

The XYZ application is currently implemented on Hewlett Packard (HP) 9000 K-Class Enterprise servers running the HP-UX 10.01 operating system. The choice of hardware is constrained by the two major services performed on the server platforms: imaging and relational database management. Since XYZ 1.0 is designed around the Wang OPEN/image product, the choice of a particular hardware component vendor and model is partially dependent on it being certified to run Wang OPEN/image Server software. To preserve the flexibility to scale server configurations, the relational database must also be available for the same hardware platform. Informix OnLine Dynamic Server (DS) for HP-UX is the current Relational Database Management System (RDBMS) used by XYZ 1.0.

The server functions can all physically reside on a single UNIX platform or be installed across multiple servers. XYZ 1.0 is currently employed across multiple servers consisting of one image server, one database server, and two clinic servers. A typical XYZ 1.0 multi-server configuration; to include standard 123 and XXX external interfaces, is depicted in Figure 1.

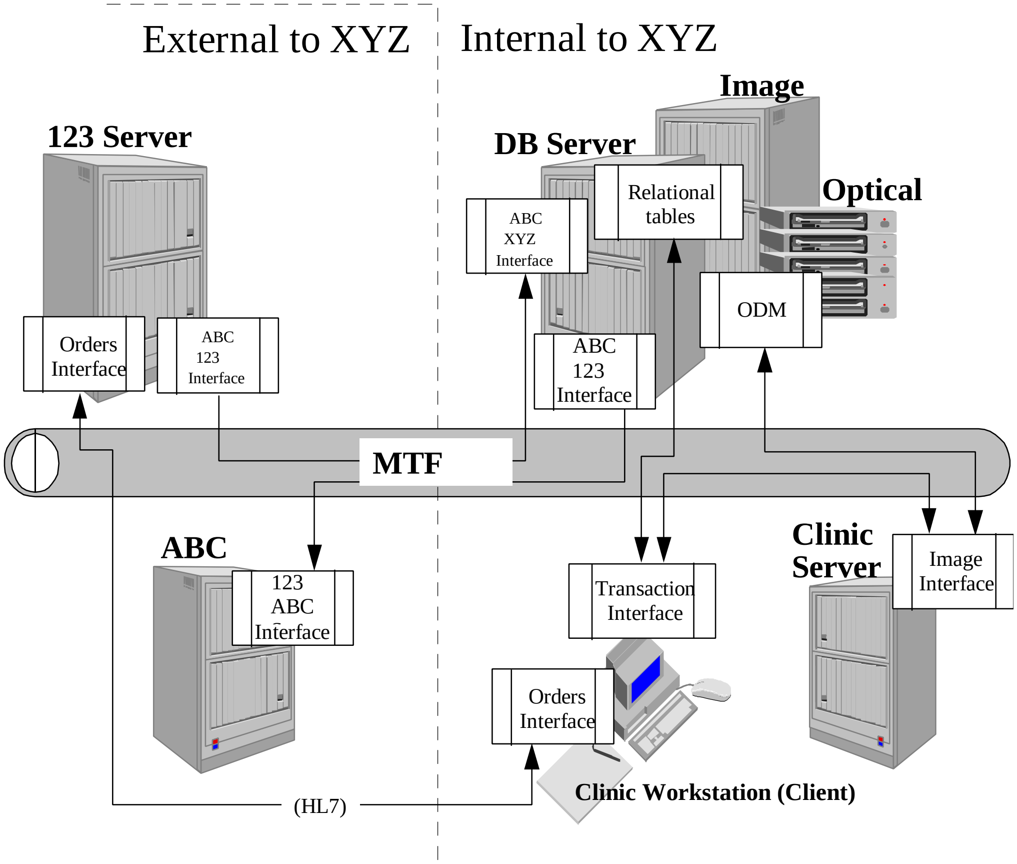

Figure 1. XYZ Version 1.0 Standard Multi-Server Configuration

Hardware configuration requirements for each server are defined in Appendix A. Table 1 describes the functional role for each XYZ 1.0 server.

Table 1. XYZ Server Functional Roles

Server	Functional Role
Image Server	The Image Server is the central repository for archived image data for XYZ 1.0. It runs the Wang OPEN/image Server product that provides store and retrieve functions for image files and stores the files on optical disks. OPEN/image integrates these services with existing UNIX services and utilities. The Distribution Manager Archiver may reside on either the Image Server or the Database Server.
Database Server	The Database Server is the central repository for clinical data retrieved from 123 and collected during patient encounters. It also maintains the index for locating image files on the optical drives and building patient histories. The XYZ 1.0 application uses the Informix OnLine DS product for its RDBMS. The Distribution Manager Archiver may reside on either the Image Server or the Database Server.
Clinic Servers	The Clinic Servers provide local image caching of image files for patients scheduled for current day appointments and retains files until completed. These servers are configured with the same executive software as the Image Server. Clinic servers store image files on magnetic disk instead of optical. Clinic servers run the OPEN/image server product, which provides storage and retrieval functions for image files and stores the files on optical disks.

Optical Storage Device

XYZ 1.0 employs the HP SureStore Optical Jukebox to provide large-capacity image storage and archiving for the image server. The jukebox, a Model 200T with a 144 slot cartridge capacity, uses industry-standard 5.25-inch, multi-function optical disks. The jukebox has four single density read/write drives. Individual disk drives can be replaced while other drives continue to read and write. The XYZ application uses 2.6 Gigabyte (GB) Write-Once-Read-Many (WORM) disk drives with 3.4 Megabyte (MB)/Sec read and 1.7 MB/Sec write speeds.

Client Hardware

Healthcare providers, administrative personnel, and system administrators use the PC client workstation to run the XYZ 1.0 application and to manage the database and imaging archive on the UNIX servers. The client hardware configuration remains the same for all these tasks since these capabilities are generally added to one of the client workstations by adding the appropriate software. The client hardware configuration includes a IBM-compatible PC, video monitor, and pen tablet, with access to a printer and laser desktop scanner. The client hardware configuration must meet the minimum requirements for running Wang OPEN/image Runtime, the XYZ 1.0 application, and the middleware utilities. Hardware configuration requirements for the XYZ 1.0 client workstation hardware components are defined in Appendix A.

XYZ Software

Server Software

The primary function of the servers is to provide central and local data management for the XYZ 1.0 application and data retrieval. The XYZ 1.0 application manages relational data and image data. HP-UX Version 10.01 is the UNIX operating system supporting all system servers. The HP-UX provides full application binary compatibility across the entire HP 9000 product line and supports Symmetric Multi-Processing (SMP). HP-UX either directly or with the addition of related products supports Transmission Control Protocol/Internet Protocol (TCP/IP) utilities, Berkley Software Distribution (BSD), Network File System (NFS) for file sharing, and Network Information Service (NIS) for network administration which are all required by XYZ 1.0. The relational data is stored in an Informix database (Informix OnLine Dynamic Server (DS) 7.2 for HP-UX) and the image data is stored on optical media managed by Wang's OPEN/image product (Wang OPEN/image Server). Because the server functions are complementary and built upon common system software (UNIX) and middleware (Informix Extended Structured Query Language (ESQL)/C containing I-NET), the logical servers can be implemented on one, two, or three physical platforms. The configuration strategy is based on the size of the MTF, performance needs, and cost. Using fewer physical platforms reduces the cost of the implementation by requiring fewer software licenses for server middleware and system software and saves on hardware costs. However, software processing requirements may reduce response times when the client accesses relational or image data. In this case, the servers' functions may be distributed on separate physical platforms and are not required to share computing resources, except for the network. Server software configurations are depicted in Appendix B.

Client Workstation Software

Microsoft Windows NT 3.51 (or higher) provides the client workstation with a multi-tasking operating environment for XYZ 1.0. Although it is designed as a 32-bit operating system, it provides preemptive multitasking for 16-bit Windows applications through its Win16 system. The application requires 16-bit emulation because the application software is built with Microsoft Visual Basic 2.0 and Visual C++ 1.52 which produce 16-bit applications. Conversion to a full 32-bit implementation will be addressed in later releases of the application. Network support for various protocols comes bundled with Windows NT. This includes the TCP/IP protocol stack and utilities used by the application and COTS software. Windows NT offers security and reliability features including account lockout and automatic reboot. The account lockout feature is the ability to set the number of unsuccessful logon attempts allowed by a user. The machine administrator can lock the user account for a pre-specified period of time, or until the administrator manually resets the account. The automatic reboot lets the user or administrator customize how the workstation reacts to a fatal system event (crash). By default, the system automatically writes the event details to the system log, alerts administrators, dumps system memory into a file that can be used for debugging, and then reboots the system.

Windows NT TCP/IP stack provides TCP/IP connectivity for the Local Area Network (LAN), for Windows NT file server access, and for the Wang OPEN/image client. Distinct TCP/IP TCP-106-VB Extensions Runtime Version 3.40 provides the Telecommunications Network (TELNET) scripting over TCP/IP used by the client application to access 123 for functions not supported by Health Level 7 (HL7) messaging. The application executes a TELNET session with 123 and supplies direct input to the 123 screen using predefined scripts. A script must be defined for every 123 screen that is to be accessed during the TELNET session. Informix I-Net Client Runtime application provides the TCP/IP connectivity between the client application and the Informix RDBMS. The Open Database Connectivity (ODBC) drivers use the I-Net Runtime for communications transport.

Intersolv DataDirect ODBC drivers provide the client application with Structured Query Language (SQL) connectivity to the RDBMS. It conforms to the Microsoft ODBC specification version 2.5 and provides a consistent level of ODBC Core, Level 1 and Level 2 function. The NT version of this driver requires a minimum of 8 Megabytes (MB) of Random Access Memory (RAM) and 6 MB of disk space (with all drivers installed). Wang OPEN/image Runtime for Windows Version 3.7.4 provides the client component of the OPEN/image Server product. The client works in conjunction with the clinic server if configured, or the central server if a single server configuration. The XYZ 1.0 application sends requests to the server to retrieve images via an Application Programming Interface (API) which then displays the image.

OPEN/image Cabinet is a stand-alone application used by system administrators to directly access the image file repository stored on the optical drives. Intersolv Data Direct Explorer provides system administrators with direct online access to the database from a client workstation. It includes an integrated set of querying, reporting, charting, and drill-down tools. System administrators may use Data Direct Explorer to run custom reports, troubleshoot data problems, and perform maintenance.

Application Software

The XYZ 1.0 application software is modular in design, uses standard interfaces (e.g., TCP/IP sockets, SQL), and relies on various COTS products for file and database communications and user interface objects. The application consists of software running on both Microsoft NT clients and UNIX server platforms. Presentation, business logic, and data access routines run on the client workstation. Custom image management and communications routines, which also perform data access, run on UNIX servers.

The XYZ 1.0 server application runs on physical UNIX servers under the HP-UX Version 10.01 operating system. The application components support patient data retrieval from 123 into the RDBMS and provide image archiving and retrieval utilities for managing image files with Wang OPEN/image. The XYZ 1.0 server application consists of the following components:

Filename	Description
DMRETRV.EXE	Distribution Manager Clinic Server, compiled in “C” under UNIX
DMARCHIV.EXE	Distribution Manager Archiver, compiled in “C” under UNIX
HOBBIT	123 Interface Server program, compiled in “C” under UNIX
XXXUNLOAD.SH	UNIX Shell script
XXXUNLOAD.SQL	DB-Access script

The XYZ 1.0 client application software runs on client Window NT 3.51 (or higher) workstations and provides the user interface for providers or medical technicians to view and record patient encounter information. The XYZ 1.0 client application software consists of the following components:

Filename	Description
PROVIDER.EXE	XYZ 1.0 program, written in Visual Basic
CODERDLG.DLL	Coder module, compiled in Visual C++
MEDSCAN.DLL	Scanning interface, compiled in Visual C++
OIBMSAVE.DLL	Encounter form conversion module, compiled in Visual C++
PR_1480.DLL	Print Patient Summary of Care module, compiled in Visual C++
MSGHANDL.EXE	XYZ 1.0 message handling program, compiled in Visual C++
PWSCOMM.VBX	XYZ 1.0 communications custom control, compiled in Visual C++

External Interfaces

The two external XYZ 1.0 interfaces are with 123 and XXX. The XYZ 1.0 application consists of two integrated databases (Informix-SQL and Wang OPEN/image); Informix-SQL stores all character data and Wang OPEN/image stores all bitmap/Tagged Image File Format (TIFF) images. The XXX and the 123 databases are closely related to the XYZ 1.0 databases. All four databases share some common data files; however, each has its own unique data sets that they use and retain. Any data that simply "passes through" the file servers and Informix-SQL database is not discussed in this section. Figure 2 shows the connectivity between the external and internal databases associated with XYZ 1.0.

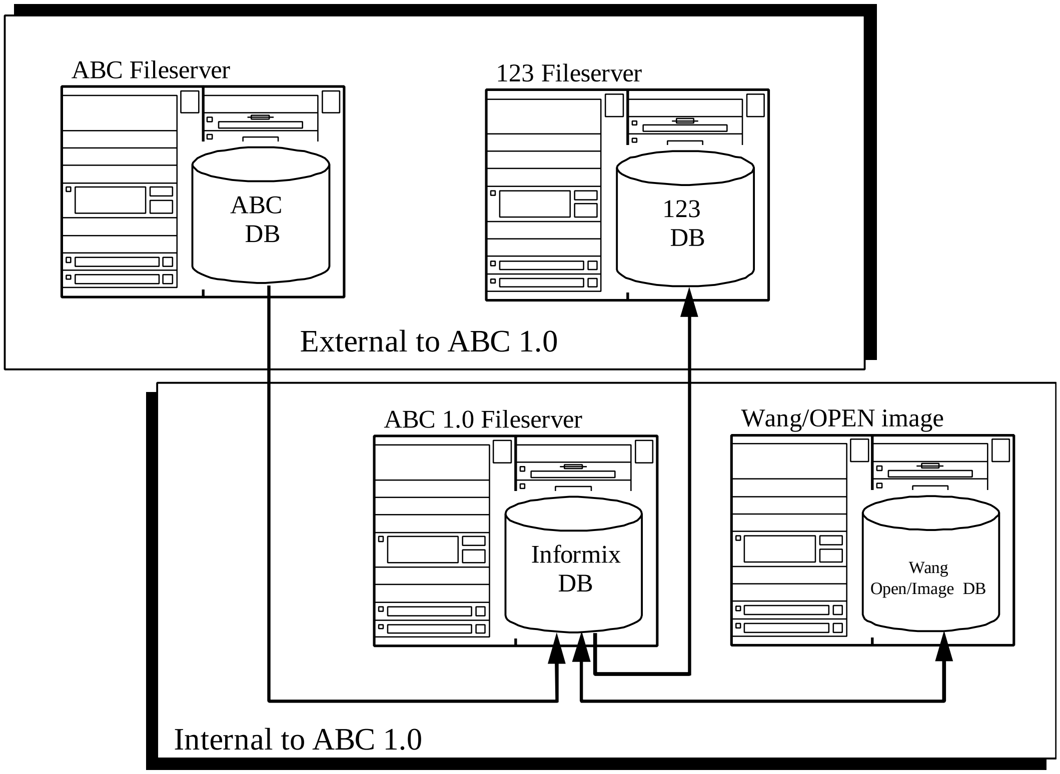

Figure 2. Database Interfaces

The XYZ 1.0 application was designed as a variant of distributed processing. In this design, data is **not** physically distributed from centralized Informix-SQL and Wang OPEN/image databases to the clinic servers. Instead, the data and screens presented to the provider at the clinic workstation are "views" from the databases placed on the clinic servers to provide improved access.

123 Interface

"Hobbit" is the 123 Interface software that communicates with the 123 Generic Interface System (GIS), via the HL7 standard interface, to provide XYZ with clinical functionality. Two types of HL7 interface transactions are supported between XYZ and 123: 1) unsolicited update interface; and 2) query/response interface.

- The unsolicited update interface is always functional for the XYZ to receive HL7 messages and update the XYZ clinical relevant database (CRDB), keeping in synchronization with the 123 database. The unsolicited updates include:

  ◊ Master File Notification: 123 notifies XYZ of various modifications made to the master files via HL7 messages;

  ◊ Results: 123 notifies XYZ of results created or received by 123; and

  ◊ Events on 123 not Initiated by XYZ: 123 notifies XYZ of various events occurring on 123 (admitting a patient, enter new orders, etc.) which are not initiated on XYZ.

- The query/response interface transactions provide a bi-directional interface via the HL7 query/response method, allowing the XYZ user to request patient information from the 123 and to enter orders. The query/response transactions include: 1)Log On; 2) Order Entry, 3) Order Management; 4) Patient Registration; and 5) Duplicate Patient Resolution.

Hobbit communicates with 123 GIS to: 1) receive the nightly download of appointment and patient data, and 2) update clinical information in the CRDB database. The nightly download of data consists of appointments scheduled for each clinic for the following day, providers assigned to the appointments, patient demographics, and applicable patient Laboratory (LAB) and Radiology (RAD) results and current medications. Hobbit populates the Informix database with the downloaded appointment and patient data, and sets the image pull indicator on the appointment list to signal the Object Distribution Manager that these patient image files are needed for the health care providers.

The query/response interface enables XYZ users (using the client workstation) to send services requests, such as clinical orders and patient query requests, into 123. Hobbit also forwards the 123 warnings and/or errors found in the order entry to the XYZ client workstation users for resolution.

XXX Interface

XXX Unload Scripts are used to transfer ambulatory information from XYZ to the XXX Server and other downstream systems, where the information is used for third party billing and other purposes. The XXX Unload Scripts perform the Informix database download functions for patient and appointment information. This information includes appointment status, ICD-9-CM codes, CPT codes, and disposition data for completed and canceled appointments and phone consults to the XXX Server. The XXX Unload Scripts contain a DB-Access script and a UNIX shell script. The UNIX shell script, XXXUNLOAD.SH, has been added to the Informix crontab, and accesses the DB-Access script. The Informix crontab automatically executes the XXXUNLOAD.SH script every night at a pre-scheduled time. The DB-Access script, XXXUNLOAD.SQL, downloads the information from the XYZ Informix database to several database unload files. These files can then be imported into an XXX Informix server for further processing. After a successful data transfer to XXX, these entries are deleted from the Appointment table and the Phone Consults tables, and the patient no longer appears on the appointment list screen in XYZ.

XYZ Philosophy of Protection

Policy Statement

As a Military Health System (MHS), the XYZ is required to implement automated system security safeguards that satisfy the requirements of DoD Directive 5200.28, DoD 5200.28-STD, and the MHS *"Automated Information System (AIS) Security Policy Manual."* XYZ system security safeguards must be designed to ensure:

- **Confidentiality** (of sensitive system data);
- **Data integrity** (system data is protected against unauthorized modification);
- **Accountability** (authorized users are held responsible for their actions); and
- **Availability** (the system and its data are available for the intended use).

Additionally, XYZ communication services are required to be properly configured to mitigate risks associated with unauthorized intrusion and modification from external system interfaces and network connections. Furthermore, procedural controls must be implemented at each MTF to ensure XYZ system security safeguards are properly implemented and maintained throughout the system's life-cycle (the required procedural controls are not addressed as part of this SDD).

Security Requirements

The following security requirements were derived from Public Law, and Federal, DoD, and Health Affairs policy on AIS security. XYZ system security safeguards were designed and implemented to meet the following requirements. The compilation of system security safeguards implemented within XYZ 1.0 establishes the XYZ TCB.

C2 Security Requirements

The following C2 security requirements were derived from DoD 5200.28-STD and serve as the foundation for XYZ system certification and accreditation. The following paragraphs provide a brief synopsis of each C2 security requirement and identify the components within XYZ that satisfy the requirement.

Discretionary Access Control (DAC)

DAC defines and controls access between users and objects (files and directories). DAC allows users to specify and control sharing of those objects and provides control to limit propagation of access rights. DAC also ensures objects are protected against unauthorized access. Access to objects by authorized users shall only be assigned by authorized users. DAC is enforced within XYZ by the HP-UX operating system, Informix RDBMS, OPEN/image, and the XYZ application. As the owner of all files and directories, XYZ system and database administrators assign user privileges during establishment of individual accounts. Access to XYZ files and directories can only be granted by individuals with system and database administration privileges. XYZ is configured to restrict unauthorized access to files and directories. In concert with current MTF business practices, access to files can be restricted to the granularity of an individual user.

Object Reuse

Object reuse ensures that all data resident in an authorized user's personal storage space be purged (rendered unrecoverable) prior to allocation of that storage space to another user. With the exception of the XYZ client workstation, users are not allocated storage space on system. Also, the XYZ application does not permit storage of sensitive data on the client workstation. Client workstations do not fall within the XYZ system boundary. Though the XYZ application resides on the client workstation, responsibility for management, control, and security of these devices resides with individuals responsible for the MTF administrative LAN. As a minimum, XYZ 1.0 requires Microsoft Windows NT Version 3.51 (or higher) be installed on the client workstation. Windows NT Version 3.51 (or higher) has been rated TCSEC Class C2 and meets object reuse requirements.

Identification and Authentication (I&A)

I&A requires all users to properly identify themselves with a unique identifier before performing any other actions. Authentication data must be protected from unauthorized access. Unique identifiers shall be used to enforce individual accountability to an associated audit event. XYZ employs a combination of user and device authentication. User authentication ensures that the individual attempting system access is an authorized user, while device authentication ensures that the user is authenticating from an authorized XYZ client workstation.

I&A within XYZ is enforced by the HP-UX operating system, Informix RDBMS, OPEN/image, and XYZ application. Authentication to XYZ is also enforced by Microsoft Windows NT on the client workstation and the 123 interface. Within XYZ 1.0, XYZ users authenticate through the XYZ application with a unique 123 identifier and are not assigned a UNIX account or unique identifiers. Consequently, XYZ users cannot log directly into the XYZ UNIX servers and are not audited within UNIX. User accountability is supported through the XYZ application as described in paragraph (4) below. UNIX accounts are established for personnel performing XYZ system administration and are audited within UNIX. In response to Software Incident Reports (SIRs), XYZ 1.0 will be modified to support XYZ user accountability within UNIX.

Auditing

Auditing provides the capability to record successful and unsuccessful events associated with individual users and the date and time the event occurs. Access to audit data must be restricted to authorized personnel and must be protected against unauthorized access and destruction. XYZ auditing is enforced by the HP-UX operating system and Informix RDBMS and is focused at recording system level events affecting system configuration and security. Events recorded by XYZ auditing include log-in attempts, administrative and privileged events, modification of file and directory discretionary access controls, and changes to the XYZ database and associated tables. XYZ audit records associate each event with a specific user and record the date and time of each successful or failed event. Access to audit data is limited to system administration personnel and is protected against unauthorized access and destruction.

System Architecture

The system architecture is designed to ensure that the security safeguards implemented within a system protects critical data (e.g., file and directory permissions, database table structure, audit records, password files, etc.) from external interference or tampering. A system's architecture must isolate the security safeguards and critical data so that they are subject to the system access control and auditing requirements. Within XYZ the system security architecture is enforced by the HP-UX operating system and Informix RDBMS. Access to system security safeguards is limited to privileged system administration personnel and is not accessible by other XYZ users. XYZ network services have been configured to restrict system access by unauthorized personnel. Access and modification of XYZ system security safeguards are captured by the system auditing function.

System Integrity

System integrity ensures that the security controls are properly configured and operating as designed by performing periodic system checks. Within XYZ system integrity mechanisms are implemented by the HP-UX operating system, Informix, and OPEN/image. Each of these COTS products performs periodic system checks to ensure proper system operation. Error messages are generated when problems are detected.

DoD Minimum Security Requirements

In addition to the above C2 requirements, XYZ system security design also satisfies the minimum security requirements derived from DoD Directive 5200.28. In many cases, an individual XYZ system security safeguard satisfies both the C2 and DoD minimum security requirements. The following paragraphs provide a brief synopsis of each applicable minimum security requirement and identify the related XYZ component that satisfies the requirement.

Accountability

Accountability ensures that security safeguards can associate system events with a specific authorized user and provide sufficient detail to reconstruct the event should a security violation or malfunction occur. Similar to system auditing, enforcement of this requirement is satisfied by HP-UX, Informix, and OPEN/image. These system components provide a detailed recording of events that can potentially degrade system performance and security. Through the use of 123 assigned Internal Entry Numbers (IEN), all XYZ user transactions within the application are accountable.

Access Control

Access control ensures that each authorized user is positively identified prior to gaining system access. All XYZ users are positively identified prior to accessing the system. Similar to I&A, XYZ enforces access control through a combination of user and device authentications. XYZ access control is enforced by the HP-UX operating system, Informix RDBMS, OPEN/image, and the XYZ application. Microsoft Windows NT on the client workstation and the 123 interface also support XYZ access control.

Sensitivity Marking

All data requires sensitivity marking to prevent unauthorized disclosure. Within XYZ the application affixes *Privacy Act* and *For Official Use Only* markings on all output products. The markings must be verified by a XYZ user for accuracy since marking cannot be depended on in a TCSEC Class C2 system.

Least Privilege

Least privilege requires that a user have access to all information to which the user is entitled, but to no more. Within XYZ the least privilege requirement is enforced by the I&A and DAC security controls. Access to data stored within XYZ and 123 functionality are limited to the privileges associated with an individual's 123 and XYZ user accounts. XYZ system administrators assign user privileges based on the business rules in force at their respective MTF.

Data Continuity

Data continuity ensures that each file or data collection has an identifiable source throughout its life-cycle. Within XYZ data continuity is enforced through the 123 interface.

Data Integrity

Data integrity ensures that safeguards can detect and minimize inadvertent modification or destruction of data, and prevent malicious destruction or modification of data. Established user permissions within the Informix and OPEN/image application prevent XYZ users from accidentally or maliciously modifying original database or image records.

XYZ Security Design

As a system employing client-server technology, XYZ security safeguards are implemented by different elements of the system. XYZ security controls were integrated to ensure protection of the system and data processed and stored by the system. The compilation of system security safeguards comprise the XYZ TCB. In addition to the security safeguards inherent to XYZ, complimentary safeguards are also provided by the 123 interface and client workstation's operating system. Complimentary safeguards are considered those security controls that are an integral part of another system but enhance the protection of XYZ. Complimentary safeguards are outside of the XYZ system boundary and are not managed or controlled by XYZ system personnel. The focus of this section is on describing the "technical controls" implemented by XYZ 1.0 to satisfy the fore-mentioned system security requirements.

Discretionary Access Control (DAC)

XYZ is an "object" based system. As an object-based system, ownership and access to all objects (e.g., files and programs) are controlled by the XYZ application. Individual users are granted privileges to access certain files based on their inclusion within a specific group. XYZ users are members of group "XYZUSER" and are granted *read*, *write*, and *execute* privileges to certain objects; however, they do not own any system objects and cannot grant access or privileges to other users. With the exception of the multi-purpose client workstation, users do not have personal storage space on the system servers. Consequently, DAC is implemented and controlled by XYZ system administrators. The following paragraphs describe how DAC requirements are enforced within XYZ 1.0 by the HP-UX operating system, Informix RDBMS, OPEN/image Application, and the XYZ application. 123 enforces DAC protection for the external interface with XYZ.

HP-UX Operating System

HP-UX 10.01 controls file access based on groups, file permissions, and file ownership. As previously stated, all sensitive files are owned by the XYZ application. XYZ users do not own files or control file access permissions. All XYZ users are members of the group "XYZUSER." File permissions associated with the "XYZUSER" group account include *read*, *write*, and *execute* privileges for files containing patient medical data stored within Informix RDBMS and OPEN/image. XYZ users are permitted access to system files through the XYZ application, but cannot authenticate or directly access files through the HP-UX UNIX operating system. Also, users are not granted system privileges to execute programs within the UNIX operating system.

Informix RDBMS

Informix system administration is limited to user(s) of group "Informix." Individuals with *root* access on the HP-UX operating system are not arbitrarily granted Informix RDBMS access or database administration privileges. The Informix RDBMS supports separation of system administrative roles to limit privileges associated with a single user. The three system administration roles supported by Informix are OnLine Database Administrator (DBA), Database System Security Officer (DBSSO), and Audit Analysis Officer (AAO). Table 2 depicts the privileges associated with each of these roles. This capability reduces the damage that could be caused by a single individual and increases traceability of any damage source. Each MTF must properly configure the Informix role separation option based on the availability of local personnel resources and security requirements.

Table 2. Informix System Administration Roles

Role	Privileges
OnLine Database Administrator (DBA)	The DBA is assigned permissions required to configure, maintain, and tune the RDBMS. Additionally, the OnLine DBA has permissions to view all data stored by the database.
Database System Security Officer (DBSSO)	The DBSSO is assigned permissions required to perform routine tasks related to maintaining the security of the RDBMS.
Audit Analysis Officer (AAO)	The AAO is assigned permissions required to configure auditing and to read/analyze the audit trail.

In addition to the role separation option described above, Informix permits restriction of user privileges at the database and table levels. Database and table level privileges are grouped into three categories: *Connect, Resource,* and *DBA*. Permissions associated with each category are listed in Table 3.

Table 3. Informix Database Privileges

Database Privilege	Authorized Functions
Connect	Execute “Select,” “Insert,” “Update,” and “Delete” statements, provided the user has the necessary table-level privileges.
	Create views, provided the user has the “Select” privilege on the underlying tables.
	Create synonyms.
	Create temporary tables and indexes on the temporary tables.
	Alter or drop a table or index, provided the user owns the table or index (or has the Alter, Index, or References privileges on the table).
	Grant privileges on a table, provided the user owns the table (or has been given privileges on the table with the “With Grant Option” keyword).
Resource	Create new tables.
	Create new indexes.
	Create new procedures.
DBA	Grant any privilege, including the DBAA privilege, to another user.
	Use the “Next Size” keyword to alter extent sizes in the system catalog tables.
	Drop any object, regardless of who owns it.
	Create tables, views, and indexes as well as specify another user as owner of the objects.
	Execute the “Drop Database” command.
	Execute the “Start Database”, and “Rollforward Database” commands.
	Insert, delete, or update rows of any system catalog table, except **systables**.

The XYZ database and all associated tables are owned by the XYZ application. XYZ users are granted database privileges associated with the *Connect* category, with the exception of altering or dropping a table or index. Currently, Informix is configured to permit all authorized XYZ users unrestricted access to database records. However, Informix can be configured to restrict access to the granularity of a single user and/or specific database table(s). User access to the Informix database and OPEN/image records can be restricted from within the XYZ application as described below.

OPEN/image

The XYZ application is the owner of all image records. XYZ users are granted *read*, *write*, and *execute* privileges for all image records. However, users do not have the permission required to modify or delete image directories or files. Within the XYZ application, users are provided a copy of the original image record that is stored separately after update or modification.

XYZ Application

XYZ enforces additional DAC protection beyond the DAC mechanisms implemented by HP-UX, Informix, and OPEN/image applications. Within XYZ, a personnel table exists within Informix that supports user authentication and restricts user access to system functions and stored data. System administrators configure the *Personnel Flag* field within the Informix personnel table to restrict an individual user's access to the patient historical medical data stored as Informix records and OPEN/image files. System administrators typically set this configuration when establishing each user's XYZ account. Based on site business rules, a MTF may restrict access to patient historical medical data based on a user's functional position (i.e., clerk, technician, etc.) or by individual user.

123 Interface

Current MTF business rules require authorized XYZ users have access privileges to all patient medical data. However, privileges to generate new patient data and modify existing patient data is limited to users with the appropriate 123 security keys. 123 security keys verify user permissions for generation and modification of patient data prior to storage within XYZ. XYZ users have restricted access to 123 data and certain functionality based on the security keys assigned when their accounts are established. Typically, each user is assigned a set of pre-established privileges associated with their relative functional position. Individual users may be issued increased or reduced privileges, as necessary, to perform their required duties. XYZ does not duplicate permissions. It defers to 123 for permissions associated with functions managed and controlled by 123 (i.e., order entry, diagnostic coding, patient treatment, etc.).

Object Reuse

XYZ users do not maintain personal data and are not allocated storage space on the UNIX servers. All data files and programs residing on the UNIX servers are owned by the XYZ application. Current MTF business rules require authorized users have access to all patient medical data residing on the system servers. Consequently, the object reuse requirement is only applicable to the multi-purpose client workstation. Object reuse on the client workstation is enforced by the Microsoft Windows NT, Version 3.51 (or higher), operating system which has received a TCSEC rating of C2. Responsibility for management, control, configuration, and certification of the multi-purpose client workstations resides with the local MTF.

Identification & Authentication (I&A)

XYZ authorized users currently obtain network and system access through a series of automated and manual log-ins. XYZ users authenticate to the HP 9000 servers through the XYZ application. Users do not log directly into UNIX and are not provided access to the UNIX command line from within XYZ. The I&A process involves successful authentication of both the user's terminal device and individual XYZ user. Future XYZ releases will reduce the number of separate authentications by evolving to a single user log-on process. The following paragraphs describe the various device and user authentication's required to access XYZ 1.0.

Client Workstation Authentication.

Users initiate the XYZ I&A process by authentication to their client workstation and local administrative network. The user's local administrative network account is required to provide word processing and printing services and is not considered a part of the XYZ internal access control process. XYZ 1.0 client application software presently resides on a workstation supported by the Microsoft Windows NT operating system. XYZ users must establish a separate account for accessing the administrative network. Each MTF is responsible for the management, access, and control of accounts associated with its local administrative network.

OPEN/image Authentication.

After successful authentication to the local MTF administrative network, users initiate the OPEN/image authentication by clicking on the XYZ Icon from the Windows NT Program Manager Screen. Authorized users input the group user-identification (ID) and password to establish the connection between the client workstation and the OPEN/image software application. Users are not provided access to XYZ data or functionality at this point.

123 Authentication.

Successful authentication to 123 is an integral part of the XYZ I&A process. Users must have a separate active 123 account, in addition to their XYZ account, to successfully complete the XYZ authentication process. 123 authentication requires a unique user-ID (Access Code) and password (Verify Code) be issued at the time the account is established. After successful authentication to the OPEN/image application, XYZ users are presented with a separate screen for authentication to 123.

Entry of the proper 123 user-ID and password initiates a sequence of automated authentication events which are required before the user can access XYZ or 123 data or functionality. The following automated authentication events (transparent to the user) are activated by a successful 123 user authentication:

- 123 returns a unique IEN to the client workstation that is forwarded to the XYZ personnel table for authentication of user data. Users not listed in the XYZ personnel table are denied system access.

- A script within the XYZ application on the client workstation forwards the application name, Internet Protocol (IP) address, and workstation name to the Informix RDBMS server for authentication.

A user is not granted access to 123 or XYZ unless the above authentications are successful. The unique IEN issued by 123 during the user's log-on process is subsequently used to authenticate various functional transactions between XYZ and 123 throughout an individual session.

Auditing

As previously stated, XYZ is an object based system and all objects (files and directories) are owned by the XYZ application. XYZ users do not maintain storage space or personal data on the system. MTF business rules require authorized XYZ users have *read* access privileges to all patient medical data. The XYZ application does not permit users to modify or delete original versions of stored data. While XYZ provides the capability to audit all user access to files it would not be efficient or realistic. XYZ auditing is implemented by the HP-UX operating system and Informix RDBMS. Auditing has been configured to record system administrator activities, changes to system security settings, and actions taken to obtain unauthorized system access. XYZ audit features can and should be configured by local MTF system administrators to selectively audit individual users if required.

HP UX Operating System

Auditing within HP-UX 10.01 is provided as part of the standard UNIX environment and trusted (secure) system. Enhanced audit capability is provided with the trusted (secure) system; however, interoperability problems with other XYZ applications prevent use of this capability. XYZ currently employs the HP-UX standard UNIX audit capability that must be manually activated and cannot be turned on through HP-UX System Administration Management (SAM). The HP-UX standard UNIX environment supports audit of all users, selected users, all events, and selected events. HP-UX provides the capability to audit:

- Administrative and privileged events;
- Object creation, deletion, opening, and closing;
- User log-ins and log-outs;
- Removable media events;
- Modifications of object DAC; and
- Access modifications other than DAC.

The HP-UX default setting records successful and failed log-ins and log-outs, modification of object DAC, and system administration events for all system users. XYZ is currently configured to audit the set of established default audit events.

Informix RDBMS

XYZ user privileges within Informix are limited to open database, issue queries, and create and place indexes on temporary tables. These activities are performed through the XYZ application. XYZ users are not granted the privileges necessary to create, modify, or delete database tables. Informix provides the capability to audit database related actions of all authorized users, individual users, selected events, or both. Informix auditing is currently configured to record successful and unsuccessful security related events and attempts to modify the database. All events initiated by the DBA, DBSSO, and AAO are also recorded. Additionally, Informix records attempts by any user to Create Roles, Set Roles, Set Session Authorization, Set Object Mode, Grant/Revoke Database Access, Grant/Revoke Table Access, Grant/Revoke Role, and Grant/Revoke Fragment Access. If required, MTFs can configure Informix to record all database related activity associated with one or more individual users.

System Architecture

XYZ 1.0 security controls that enforce system architecture requirements are implemented by the HP-UX operating system and Informix RDBMS COTS applications. The following paragraphs provide a brief description of these security controls.

HP UX Operating System

Within the HP-UX system architecture, requirements are met by security controls that restrict access to the system, system files, and system processes. These files are considered critical system files that directly support the HP-UX operating system and are not an integral part of the XYZ application. The HP-UX operating system enforces system access by requiring users to authenticate with a unique user-ID and password. The HP-UX operating system restricts user access to system files based on file permissions (e.g., *read*, *write*, and *execute)* assigned by the file owner or an individual with *root* access. XYZ users are not granted file permissions to critical system files. Execution of HP-UX system processes is restricted to those users with *root* permissions. The HP-UX operating system also provides the capability to audit each user’s access, modification, and deletion of system files. The XYZ 1.0 HP-UX operating system is presently configured to audit all system log-ins, changes to DAC settings, and actions performed by a system administrator.

Informix RDBMS

In addition to the security access controls implemented by by the HP-UX operating system, Informix enforces application, database, and table access controls. The Informix application is partitioned so as to operate independent of the HP-UX operating system. HP-UX system administrators, operators, and users must be granted appropriate permissions to access the Informix database application. Within Informix, database administrators manage access to a specific database and its associated tables. Users require database *root* level permissions to perform administrative or privileged functions within Informix. Access to and modification of Informix security safeguards are restricted to users with database *root* level permissions. Within XYZ 1.0, Informix is configured so that users have limited privileges to generate and modify table records through the XYZ application. Informix also supports audit of application access and actions by database users. Within XYZ 1.0, Informix is presently configured to record database administration type actions.

System Integrity

XYZ system integrity is supported by automated and semi-automated features within the HP-UX operating system, Informix RDBMS, and OPEN/image. A brief description of these features is described in the following paragraphs.

HP-UX Operating System

The HP-UX operating system performs periodic automated system checks in the form of system calls as part of the audit function. System administrators can select from an extensive list of system calls that periodically check system security related functions. Successful and failed system calls are recorded in the audit log. In addition to system calls system administrators can execute the command *fsck*. The *fsck* command audits and interactively repairs inconsistent conditions for HP-UX file systems on mass storage device files. If the file system is consistent, the number of files on that file system and the number of used and free blocks are reported. If the file system is inconsistent, *fsck* provides a mechanism to fix these inconsistencies.

Informix RDBMS

Informix employs various tools and utilities (i.e., message log, system console, On-monitor, SMI tables, onstat utility, oncheck utility, and onperf utility) to monitor and report on the correct operation of the RDBMS. Most of the tools perform continuous monitoring and periodic reporting to the database administrator's terminal. System status monitoring supported by Informix utilities must be initiated by users with database *root* equivalent privileges.

OPEN/image

OPEN/image system integrity is maintained by the Server Management Services which is accessible to users with *root* permissions through the OPEN/image Server Utility (OIUTIL). The Server Management Services provide system administrators with the capability to start up, control, monitor, and terminate all image services. Each installed image service logs event and information messages to a central log file on the image server. System administrators can view the event status for all services through the Event Log screen.

Accountability

In addition to the formal audit capability described above, accountability of user actions is also enforced by the OPEN/image application and 123 interface. The following paragraphs describe the process for ensuring user accountability.

OPEN/image Application

Within OPEN/image authorized users can only view and create image records. XYZ users cannot modify or delete stored original graphic image records. Users are provided a copy of the original image record that can be modified and stored as a new record. The XYZ application requires each image copy be signed by the individual generating the record prior to its storage. This capability provides traceability for image related transactions. The audit capability within OPEN/image is limited to recording system status (event) messages for the various software application services (i.e., document management service, image file service, image security service). Events recorded for each application service include: debug (most logging), information, notice, warning (default), error, critical, alert, and emergency (least logging). These events are grouped into three categories: most logging, default, and least logging. XYZ was configured to capture the events associated with the default and least logging categories.

123 Interface

All Informix files and OPEN/image records stored within XYZ contain a unique IEN assigned by 123. The unique 123 IEN is assigned to all transactions (e.g., database records and image files) generated by a specific user while logged onto the system. XYZ system administrators can easily identify the originator of each stored database record or image file. This capability permits accountability of user actions without generating a large amount of audit data.

Access Control

Access controls within XYZ are enforced by the DAC and I&A processes described above. Additional access controls are enforced by the HP-UX operating system.

- The HP-UX operating system enforces access control for all data stored on the XYZ servers. Currently authorized XYZ users initiate system access through the XYZ application and do not perform a UNIX log-in. Authorized XYZ users cannot perform functions outside of the XYZ application as they do not have a UNIX account.

- System personnel (i.e., system operators, database administrators, system security personnel, etc.) are assigned individual UNIX accounts and must log-in to the HP-UX operating system, Informix RDBMS, and OPEN/image application with a unique user-ID and password. XYZ audit is targeted at capturing the events performed by system personnel. While system personnel have access to the raw data stored in the Informix RDBMS and OPEN/image application, assimilation of this sensitive information is impractical outside of the XYZ application.

- In addition to the access controls enforced by system authentication; all unnecessary network services (i.e., mail, anonymous File Transfer Protocol (FTP), Trivial File Transfer Protocol (TFTP), etc.) have been deactivated and remaining network services configured to reduce the potential for unauthorized system access. In the event of an unauthorized intrusion, system audit records the malicious activity.

Sensitivity Marking

The XYZ 1.0 application automatically affixes *Privacy Act* and *For Official Use Only* markings on all output products; however, these markings must be physically verified by a XYZ user as their accuracy cannot be depended upon in a TCSEC Class C2 system.

Least Privilege

Within XYZ least privilege is enforced by a combination of the HP-UX operating system, Informix RDBMS, OPEN/image application, 123 interface, and XYZ application. The system security controls described above in support of DAC also satisfy the least privilege requirement.

Data Continuity

Within XYZ an IEN generated by 123 is assigned to all stored data and image records throughout their life-cycle. The 123 assigns an IEN to each user transaction and directly associates the initiating user with each transaction.

Data Integrity

Within XYZ data integrity is enforced through the Informix RDBMS, OPEN/image application, and 123 interface. XYZ users may only access data stored in Informix and OPEN/image through the XYZ 1.0 application. XYZ users may only access data stored in Informix and OPEN/image through the XYZ 1.0 application. XYZ user privileges within the Informix database are limited to *connect*. *Connect* privileges do not permit users to delete previously stored data. XYZ users maintain similar type privileges within OPEN/image. Users are provided a copy of original image records for update and cannot modify or delete original image records. Accidental or malicious modification or deletion of original database and image records can only be performed by individuals with *root* privileges. 123 is the source of over fifty percent of the data resident in XYZ (i.e., pharmacy orders, radiology orders, laboratory orders, consultation orders, clinical orders, ancillary orders (scheduled and non-scheduled), test results, examination results, patient identification, etc.). This data remains resident in XYZ and 123 in the event of suspected data corruption.

Appendix A
Hardware Configuration

A-1. Image Server Hardware

Table A-1 defines the XYZ 1.0 Image Server hardware configuration requirements proposed for the XYZ AFB MTF.

Table A-1. Image Server Hardware Configuration

Central Processing Unit	• Hewlett Packard (HP) 9000 K200
Memory	• 256 MB Error Checking and Correcting (ECC) Memory
Disk Storage	• 2 GB Fast/Wide/Differential (FWD) Standard Computer Systems Interface (SCSI)-2 Disk Drive (Qty 3) • HP-Precision Board (PB) FWD SCSI-2 Host adapter • Quad speed Compact Disk-Read Only Memory (CD-ROM) drive
Optical Storage	• HP Surestore optical 200T jukebox • HP 2.6 GB Write-Once-Read-Many (WORM) optical disk (Qty 2)
Tape Storage	• 4GB Digital Data Storage (DDS) Digital Audio Tape (DAT) Drive w/compression
Network Interface Card	• LAN/9000 link for HP-PB Based servers and Local Area Network (LAN) card • System and Network configuration
System Console	• Monochrome, Green
Other Hardware	• Rack mount kit for HP 3000/9000 K class • 1.6 meter standard Electronics Industries Association (EIA) Rack

A-2. Database Server Hardware

The Database Server capacity is dependent on the resource consumption of the database management software and functions, size of the data, number of connections, table space, and transaction frequency. In addition, server application software including the 123 Interface server (Hobbit) and the Distribution Manager Archiver, which access the database, also resides on this server. Table A-2 defines the XYZ 1.0 Database Server hardware configuration requirements proposed for the Scott AFB MTF.

Table A-2. Database Server Hardware Configuration

Central Processing Unit	• HP 9000 K420, dual processor
Memory	• 256 MB ECC Memory
Disk Storage	• 2 GB FWD SCSI-2 Disk Drive (Qty 2) • 20 MB FWD SCSI-2 Interface (Qty 2) • Quad speed CD-ROM drive • HA Storage system factory rack enclosure • 2x2 1 GB FWD high performance disk module
Tape Storage	• 4GB DDS DAT Drive w/compression
Network Interface Card	• LAN/9000 link for HP-PB Based servers and LAN card • System and Network configuration
System Console	• Monochrome, Green
Other Hardware	• K400 4 HP-HSC slot expansion upgrade • 1.6 meter standard EIA Rack • Redundant hot pluggable power supply

A-3. Clinic Server Hardware

The Clinic Servers run the same OPEN/image server product as the Image Server but do not have an attached optical jukebox. Instead, these servers cache images retrieved from the Image Server for access by the client workstations. Table A-3 defines the XYZ 1.0 Clinic Server hardware configuration requirements proposed for the Scott AFB MTF.

Table A-3. Clinic Server Hardware Configuration

Central Processing Unit	• HP 9000 K200
Memory	• 256 MB ECC Memory
Disk Storage	• 2 GB FWD SCSI-2 Disk Drive (Qty 2) • 20 MB FWD SCSI-2 Interface • Quad speed CD-ROM drive • HA Storage system factory rack enclosure • 2x2 1 GB FWD high performance disk module
Tape Storage	• 4GB DDS DAT Drive w/compression
Network Interface Card	• LAN/9000 link for HP-PB Based servers and LAN card
System Console	• Monochrome, Green
Other Hardware	• 1.6 meter standard EIA Rack • Rack mount kit for HP 3000/9000 K class • Redundant hot pluggable power supply

A-4. Client Workstation Hardware

XYZ 1.0 Client Workstation hardware components include an IBM-compatible PC, video monitor, printer, laser desktop scanner and pen tablet. Table A-4 displays a typical client workstation with the configuration recommended by the XYZ development team, which is appropriate for any size MTF.

Table A-4. Client Workstation Hardware Configuration

Central Processing Unit	• IBM-compatible Pentium 100 MHz or greater
Memory	• 32 MB Random Access Memory (RAM)
Disk Support	• 2 GB SCSI hard drive • 1.44 MB floppy disk drive
Monitor	• Cornerstone Color 20/70 monitor and Image Accel 2 Controller, or Intergraph Monitor with Image Accel 2 Controller
Pen or Mouse Device	• Wacom ArtPad II, CalComp Tablet, or 2-button mouse
Scanner	• HP Scanjet 4C Color Scanner or equivalent
Network Interface Card	• Network interface card supporting Institute of Electrical and Electronic Engineers (IEEE) 802.3, 10 Mbps

Appendix B

Software Configuration and Architecture

B-1. Image Server Software

The Image Server is the central repository for archived image data for XYZ 1.0. It runs the Wang OPEN/image Server product which provides store and retrieve functions for image files and stores the files on optical disks. OPEN/image integrates these services with existing UNIX services and utilities. The Informix ESQL/C runtime is used by the Distribution Manager Archiver as database and communications middleware for its SQL calls to the database server. Table B-1 depicts the Image Server software configuration.

Table B-1. Image Server Software Configuration

System Software	• HP-UX Version 10.01 operating system • Wang OPEN/image Optical Disk (OD) Standalone/Jukebox driver for 1.3 HP-UX (comes with server software)
Middleware	• Informix 7.2 ESQL/C Runtime for HP-UX • HP-UX TCP/IP
Imaging Software	• Wang OPEN/image Server for HP-UX
XYZ 1.0 Application Software	• XYZ 1.0 Distribution Manager Archiver application

(Note: The Distribution Manager Archiver application may reside on either the Image Server or the Database Server. Informix I-Net is now packaged with Informix QL/C).

Figure B-1 depicts the Image Server software architecture.

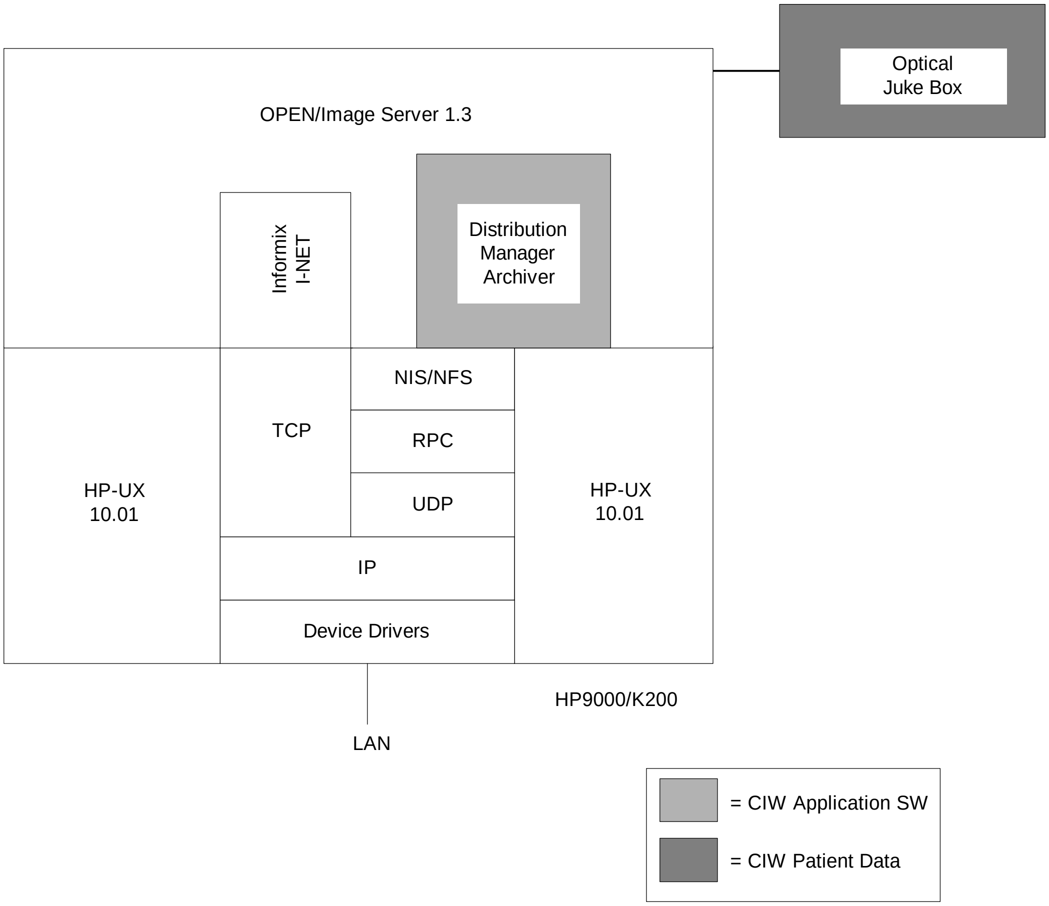

Figure B-1. XYZ Image Server Software Architecture

B-2. Database Server Software

The Database Server is the central repository for clinical data retrieved from 123 and collected during patient encounters. It also maintains the index for locating image files on the optical drives and building patient histories. The XYZ 1.0 application uses the Informix Dynamic Server product for its RDBMS. Informix ESQL/Runtime provides the database middleware to support SQL calls made by the XYZ 1.0 123 Interface Server (and Distribution Manager Archiver, if implemented on this platform). Table B-2 depicts the Database Server software configuration.

Table B-2. Database Server Software Configuration

System Software	• HP-UX Version 10.01 operating system
Middleware	• Informix 7.2 ESQL/C Runtime for HP-UX • HP-UX TCP/IP
Database Software	• Informix 7.2 Online Dynamic Server (DS) Runtime for HP-UX
XYZ 1.0 Application Software	• XYZ 1.0 123 Interface Server (Hobbit) application

(Note: The Distribution Manager Archiver application may reside on either the Image Server or the Database Server. Informix I-Net is now packaged with Informix 7.2 ESQL/C).

Figure B-2 depicts the Database Server software architecture.

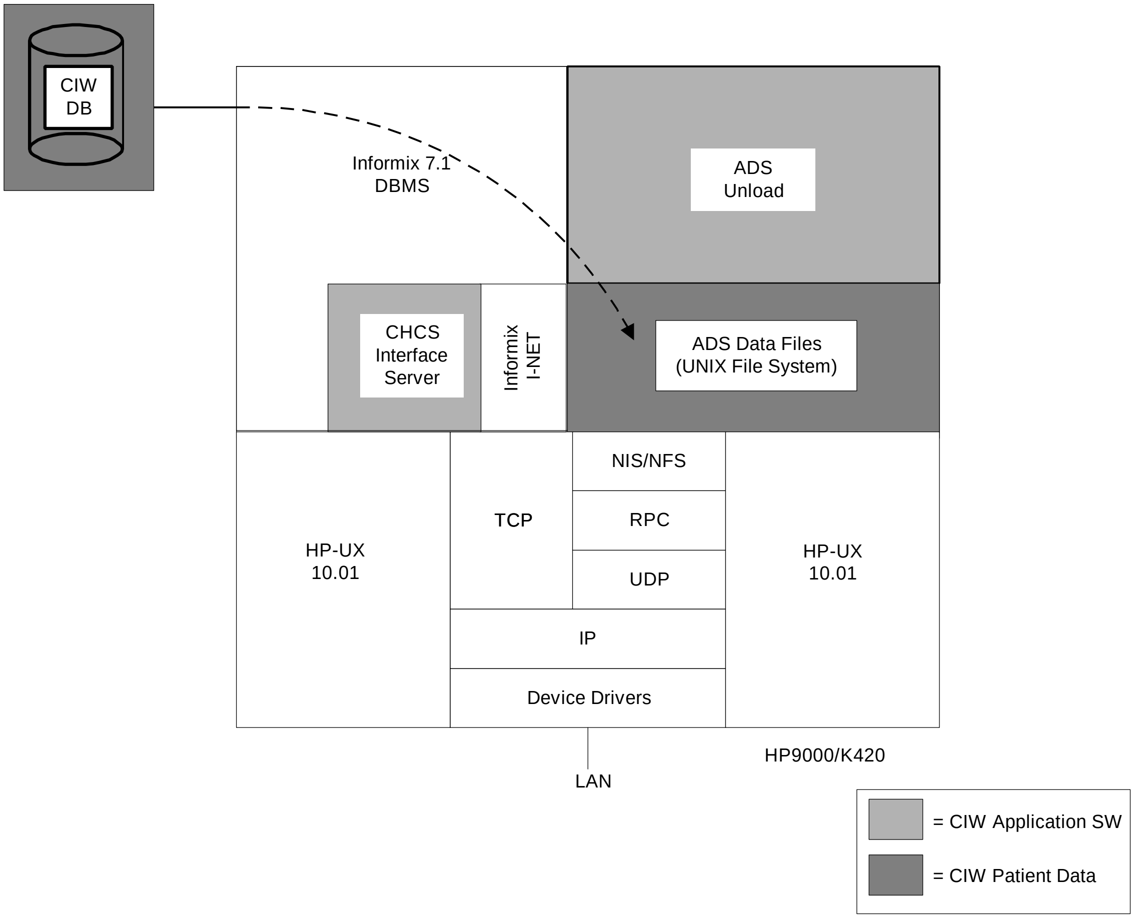

Figure B-2. XYZ Database Server Software Architecture

B-3. Clinic Server Configuration

The Clinic Server provides local image caching of image files for patients scheduled for current day appointments and retains files until completed. This server is configured with the same executive software as the Image Server; however, it stores image files on a magnetic instead of optical disk. The Distribution Manager Server application uses Informix ESQL/C as the central repository for archived image data for XYZ 1.0. It runs the Wang OPEN/image Server product, which provides storage and retrieval functions for image files and stores the files on optical disks. OPEN/image integrates these services with existing UNIX services and utilities. Informix ESQL/Runtime provides the database middleware to support SQL calls made by the XYZ 1.0 123 Distribution Manager Server. Table B-3 depicts the Clinic Server software configuration.

Table B-3. Clinic Server Software Configuration

System Software	• HP-UX Version 10.01 operating system
Middleware	• Informix 7.2 ESQL/C Runtime for HP-UX • HP-UX TCP/IP
Imaging Software	• Wang OPEN/image Server for HP-UX
XYZ 1.0 Application Software	• XYZ 1.0 Distribution Manager Server application • Medical clip art

Figure B-3 depicts the Clinic Server software architecture.

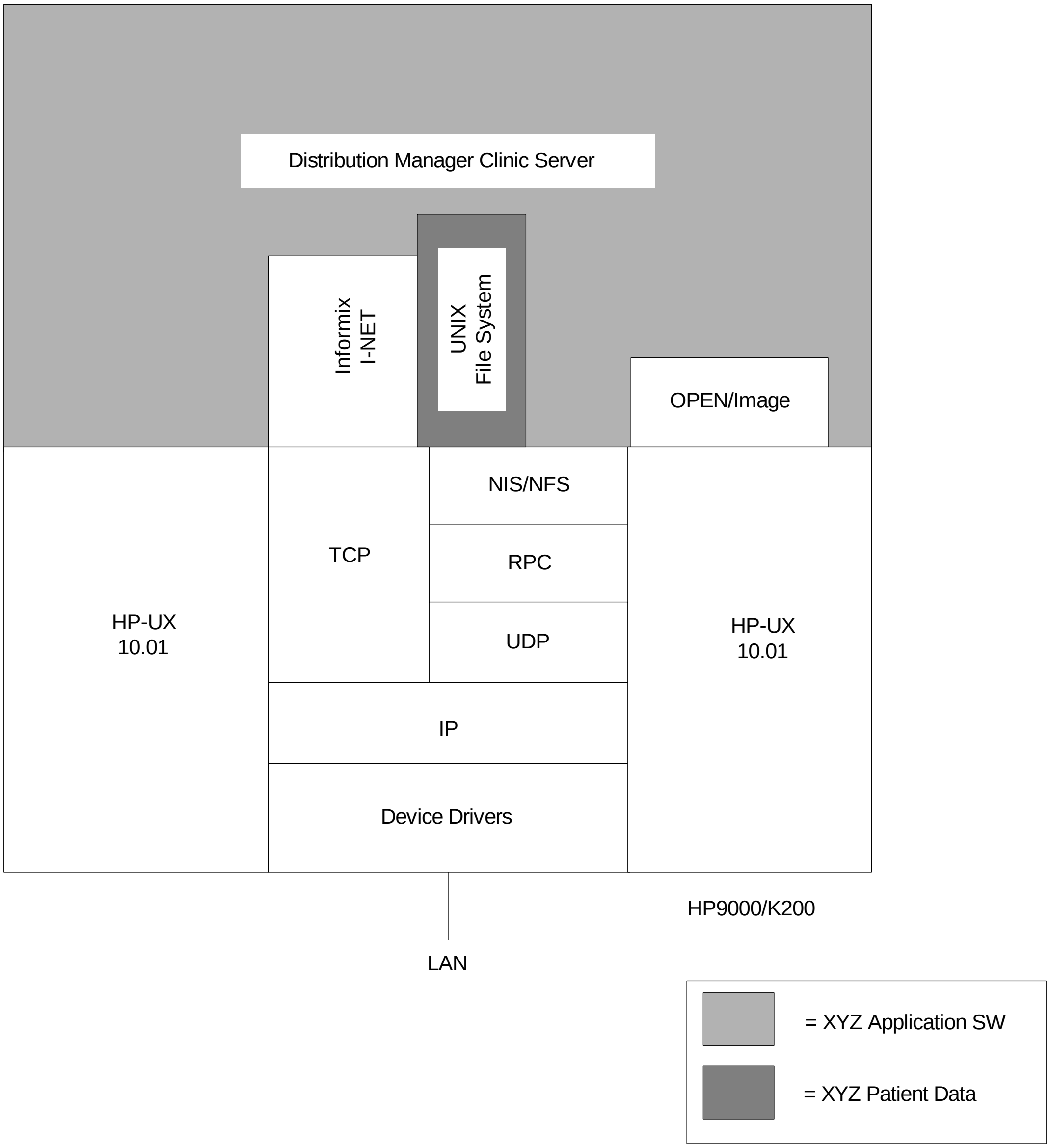

Figure B-3. XYZ Clinic Server Software Architecture

Attachment 3 - Preparation Guide for Draft Core SSAA

Military Health Services Automated Information Systems Program

System Security Authorization Agreement Preparation Guide

HEALTH AFFAIRS

Prepared By:
Military Health Services
Automated Information Systems Security Team
5111 Leesburg Pike Suite #302
Falls Church, VA 22041

1.0. Preface

This document provides information regarding the preparation of a System Security Authorization Agreement (SSAA), in accordance with (IAW) Department of Defense (DoD) Instruction 5200.40, *Defense Information Technology Security Certification and Accreditation Process (DITSCAP)*, December 30, 1997. The document includes a suggested outline for a SSAA and a description of the information contained in each section. This document is provided as a guideline for preparing a SSAA as part of the automated information system (AIS) or network certification and accreditation (C&A) process. Additional information regarding the SSAA can be found in DoD Instruction 5200.40 and the DITSCAP Implementation Guide. Personnel preparing the SSAA should read and understand the DoD Instruction 5200.40 and the DITSCAP Implementation Guide prior to preparing the SSAA. The DoD Instruction 5200.40 and the DITSCAP Implementation Guide are referenced in this document and should be used in conjunction with this document.

2.0. Introduction

The SSAA is a living document that represents the formal agreement among the Designated Approving Authority (DAA), Certifying Authority (CA), User Representative, and Program Manager. The SSAA is used throughout the entire DITSCAP to guide actions, document decisions, specify Information Technology Security (ITSEC) requirements, document certification tailoring and level of effort, identify potential solutions, and maintain operational systems security. The primary objectives of the SSAA are provided below:

- Document the formal agreement among the DAA(s), the CA, the user representative, and the program manager.
- Document all requirements necessary for accreditation.
- Document all security criteria for use throughout the IT system life cycle.
- Minimize documentation requirements by consolidating applicable information into the SSAA (security policy, concept of operations (CONOPS), plans, architecture description, etc.).
- Document the DITSCAP plan.

The SSAA is developed in Phase 1 and updated in each phase as the system development progresses and new information becomes available. The SSAA consolidates the system and security documentation into one document. This eliminates redundancy and potential confusion as multiple documents describe the system, security policy, system and security architecture. When feasible, the SSAA can be tailored to incorporate other documents as appendices or by reference to the pertinent document. A suggested outline of the SSAA is provided in Enclosure 2.

The completed SSAA contains those items agreed to by the DAA, CA, User Representative, and Program Manager. The support organizations must understand each of these essential items.

3.0. SSAA Outline Detailed Descriptions

The following information defines the contents of each section of the suggested outline of the SSAA. References to other documents for more detailed information and suggested charts are provided.

3.1. Mission Description and System Identification. This section describes the system and the mission that the system supports. This includes a statement on how the system supports the organization's mission, the name of the organization, the system's name, the length and stage of the system within its life cycle, a discussion of the information categories to be processed to support the mission, a high level information flow specification, a functional description, a statement on personnel clearances, and a stipulation of the system criticality. The mission description is a concise, high-level system specification and needs statement. It describes whom the system will serve, how it will work, what information it will process, how important it is, and why it is being developed. It does not contain implementation specifics. The DITSCAP Implementation Guide, Section 3, C3.3.2, provides additional details on how to prepare this section.

3.1.1. System Name and Identification. This section identifies the system being developed or entering the C&A process. This section provides the name of the system, the name of the organization that owns the system, and the organization name of the ultimate user. It identifies the general user, which helps to define operational scenarios that may be encountered, especially for tactical systems.

3.1.2. System Description. This section provides a complete high-level description of the system architecture. Diagrams or drawings should be included to clarify the description. All components of the system should be described. If the information is insufficient or the understanding of the system is insufficient for the system description to be written, the system is not ready to begin the C&A process.

3.1.3. Functional Description. This section provides a summary of the system functionality. More detailed information should be provided in Appendix G (System Architecture). Provide the purpose and functional description of the system. Describe functions performed jointly with other systems and identify the other systems. Include high level functional diagrams. Provide the intended flows of data into the system, data manipulation, and output of the resultant products. The mission need should clearly state the purpose for which the system is needed and the capabilities desired.

3.1.3.1. System Capabilities. This section provides a brief statement explaining the capabilities of the system. The system capability information provides a summary of the system mission and function statements. The system capability description should clearly delineate what function or capability is expected to be present in the fully accredited system.

3.1.3.2. System Criticality. This section examines the consequences of a loss of the system. It assesses the affect upon operations of the DoD, the various Military Departments, or other government agencies if they were denied the reliable use of this system. From this analysis, a determination of the system's criticality is made.

3.1.3.3. Classification and Sensitivity of Data Processed. This section states the highest classification of information intended for processing on the system (unclassified, sensitive unclassified, confidential, secret, top secret) along with any special compartment or subcompartments. The information category is also to be used to determine the overall system class. This requires the identification of the type of information processed (Privacy Act, financial, critical operational, proprietary, and administrative).

3.1.3.4. System User Description and Clearance Levels. The security architecture, level of security assurance, and security design requirements depends a great deal on the security clearances of users, their access rights to the specific categories of information processed, and the actual information the system is required to process. Therefore, it is essential that the mission need clearly state the user population's security clearances and access rights to other restricted information. For example, a system may be required to have contractor personnel as authorized users; however, under classification of data processed, the mission need states that proprietary information from commercial organizations other than the users would be processed. This situation creates a security problem in that sufficient controls must be designed into the system to preclude having the contract users gain intentional or unintentional access to the proprietary data.

3.1.3.5. Life cycle of the System. This section describes the life cycle program and where the system is in relationship to its life cycle. For example, if the mission need states that a sensor support system is needed urgently to provide tactical support to ongoing operations, an accelerated development and acquisition process is most likely to be used. The C&A process must be prepared to keep pace with this effort, and this may require resource allocation on the part of the CA and DAA.

3.1.4. System CONOPS Summary. This information supplements the system description and function statements. This section should provide a high level description of the concept for the system to satisfy the mission need. Provide a description of those functions that are jointly performed with other systems, and identify the other systems.

3.2. Environment Description. This section documents the intended operational environment, software development and maintenance environment, the threat environment, and external electronic connections. This will include the connection layer information. If more than one location is used, provide details for each in a separate section. The DITSCAP Implementation Guide, Section 3, C3.3.3, provides additional details on how to prepare this section.

3.2.1. Operating Environment. This section identifies and describes the physical environment in which the system will operate, including floor plans, equipment placement, electrical and plumbing outlets, and telephone outlets. Describe the access control procedures provided by the environment and any other standard operating procedures that support a secure environment. Include existing security features mandated by the operational situation in this section. Provide a description of the existing environmental security features that will mitigate the implementation of specific security requirements in that environment rather than in the system architecture and design.

3.2.2. Software Development and Maintenance Environment. This section identifies and describes the software development and maintenance environment, open or closed. A closed security environment is an environment where the security clearance and information access, and configuration control requirements specified in the DITSCAP Implementation Guide, Section 3, table C3-6 are satisfied. An open environment is an environment that does not satisfy the conditions of a closed environment. The DITSCAP Implementation Guide, Section 3, C3.3.2, provides additional details for the development of this section.

3.2.3. Threat Description. This section defines the potential threats to the system. The definition shall consider the intentional and unintentional events that can affect the integrity, confidentiality, and availability of the system. Unintentional human error, system design weaknesses, and intentional actions on the part of authorized as well as unauthorized user can cause these events to occur. Identify and describe the vulnerability-induced threats, environmentally based threats, and the impact these threats have on mission

need. The DITSCAP Implementation Guide, Section 3, C3.3.3.3, provides additional information for the development of this section.

3.3. System Architectural Description. This section provides summary information describing the system architecture. Detailed information should be provided in Appendix G (System Architecture). The architecture description provides the framework for the information system architecture and includes a physical description of the hardware, software, firmware, and interfaces. Against this framework, the architecture description stipulates the security architecture. Existing or planned system features that facilitate expansion or external connection should be mentioned in this section. During the concept development phase, the architecture may not be fully developed. A broad description of these areas may be provided. However, once the information system has entered the design phase, the architecture description must be updated and details filled in. Areas may exist that do not apply to the information system (e.g., firmware). For such an instance, it is appropriate to enter the term "nonapplicable." Adequate detail should be included to compare the system's architecture with the Technical Architecture Framework for Information Management (TAFIM) Volume 6, Defense Goal Security Architecture (DGSA). The DITSCAP Implementation Guide, Section 3, C3.3.4, provides additional information for completing this section.

3.3.1. Hardware. This section identifies and describes the hardware used and whether it is a standard commercial product, unique, or on the National Security Agency (NSA) Evaluated Products List (EPL). Hardware is the physical equipment as opposed to programs, procedures, rules, and associated documentation. If this development effort involves an existing hardware change, identify the specific hardware components being changed. Include an equipment list and describe the target hardware and its function as part of Appendix G (Security Architecture).

3.3.2. Software. This section identifies and describes the operating system(s), database management system(s), and applications. Software includes the entire set of application programs, software procedures, software routines, and operating system software associated with the system in question. This includes manufacturer supplied software, other commercial off-the-shelf software, and all programs generated applications software. The features of any security packages used on the system should be identified and describe in Appendix G (Security Architecture). Identify any software packages that are commercial off-the-shelf (COTS), government off-the-shelf (GOTS), and on the EPL and describe the target software and its intended use.

3.3.3. Firmware. This section identifies and describes the firmware used and whether it is a standard commercial product, unique, or on the EPL. For example, items such as programmable read-only memory (PROM) and enhanced PROM (EPROM) devices are considered firmware. The software that is stored permanently in a hardware device that allows reading and executing the software, but not writing or modifying it should be described in Appendix G (Security Architecture).

3.3.4. System interfaces and external connections. This section provides a statement of the significant features of the communications layout. A high level diagram of the communications links and encryption techniques connecting the components of the information system, associated data communications, and networks should be included in Appendix G (Security Architecture). Appendix G should describe the system’s external interfaces. The description should include a statement of the purpose of each external interface and the relationship between the interface and the system.

3.3.5. Data flow. This section describes the system's internal interfaces and data flows. The types of data and the general methods for data transmission should be stated if specifically required. Diagrams or text to

explain the flow of critical information from one component to another should be included in Appendix G (Security Architecture). From this the security engineer, working with the Program Manager, can make an initial assumption on a suitable method for processing the data flow requirements.

3.3.6. DGSA Security View. This section provides a statement of the relationship of the system architecture to the DGSA. The DGSA has been designed to promote interoperability and conserve resources. A comparison of the significant features of the system's architecture to the DGSA should be provided in Appendix G (Security Architecture). Include a diagram of the relationship of the system architecture to the DGSA.

3.3.7. Accreditation Boundary. This section provides a statement of the boundary of the system. Diagrams or text to clearly delineate components to be evaluated as part of the C&A should be included in Appendix G (Security Architecture). All components included shall be described in the systems description. Elements outside the accreditation boundary shall be included in the description of the external interfaces.

3.4. ITSEC System Class. This section and subsections provide information for determining the system class of the system. The DITSCAP Implementation Guide, Section 3, C3.3.8.2 and Appendix 4 provide additional information for determining the system class. Reading the DITSCAP Implementation Guide Appendix 4 is highly recommended for completing this section of the SSAA. This section should contain a completed ITSEC Characteristic Chart. An example of an ITSEC Characteristic Chart is provided in Exhibit 1.

Characteristic	Operation	Data	Infrastructure	System	Alternatives
Interfacing Mode					Benign, Passive, Active
Processing Mode					Dedicated, Compartmented, System High, Multi-level
Attribution Mode					None, Rudimentary, Selected, Comprehensive
Mission-Reliance Factor					None, Cursory, Partial, Total
Accessibility Factor					Reasonable, Soon, ASAP, Immediate
Accuracy Factor					Non-Applicable, Approximate, Exact
Information Categories					Unclassified, Sensitive Information, Collateral Classified, or Compartmented/Special Access Classified

Exhibit 1: ITSEC Characteristics Chart

The ITSEC class decision process begins by considering the impact of the system on other systems. It then considers system user interaction, mission, and data types. To consider the impact on other systems, one must assess the risk of the specific system to other systems. This approach to ITSEC evaluation, C&A, focused on infrastructure, determines the universal risk to other systems, not just the specific system under consideration. The ITSEC class resolves several security discriminating characteristics for a system by first considering the same characteristics for the operation and data associated with the system. This is done with direct consideration of the infrastructure where the system is connected. The characteristics for the system must be chosen to be adequate to accommodate the operation, the data, and associated infrastructure considerations. The characteristics include interfacing mode, processing mode, attribution mode, accessibility factor, accuracy factor, and information categories. Specific alternatives for each characteristic are provided in the section 4 subsection. Detailed descriptions are provided in the DITSCAP Implementation Guide, Appendix 4, AP4.2.2 - AP4.2.8.

The system class is determined by first selecting an applicable alternative for each system characteristic for operations, data, and infrastructure. The first three columns of the ITSEC Characterization Chart should be completed. Next the first three entries are resolved to reflect the most applicable value for the fourth column so that the system will adequately support the needs defined in the first three columns. This will result in a system with the minimum security requirements required in the context of its associated operation, data, and infrastructure. Each subsection in section 4 of the SSAA should provide the determined alternative and the rationale for selecting the alternative for operations, data, and infrastructure.

The system class is used to specify the level of effort for system certification. The certification level is used to scope the certification tasks performed in Phases 2 and 3 of the DITSCAP.

3.4.1. Interfacing mode. This section provides the selected interfacing mode and the rational for selecting the mode. The interfacing mode categorizes interaction. The question concerns containment of risk, (e.g., if a problem were to occur with the operation, data, or system, what would be the risk to other operations, data, or systems with which it interacts). The interactions of systems may be through physical or logical relationships. These relationships are referred to as benign, passive, or active**.**

3.4.2. Processing mode. This section provides the selected processing mode and the rational for selecting the mode. The processing mode distinguishes the way processing, transmission, storage, or data is handled. It reflects the use of the system by one or more different sets of users or processes. The alternatives are dedicated level, system high level, compartmented level, and multi-level. **Each of the modes exhibits unique security qualities.**

3.4.3. Attribution mode. This section provides the selected attribution mode and the rational for selecting the mode. The attribution mode distinguishes the degree or complexity of accountability required to establish authenticity and nonrepudiation. Four alternatives are none, rudimentary, selected, and comprehensive**.**

3.4.4. Mission-reliance factor. This section provides the selected mission-reliance factor and the rational for selecting the factor. The mission-reliance factor relates the degree to which the success of the mission relies on the operation, data, infrastructure, or system. The criticality of the mission in a broader context is independent of that factor and is used separately. Four alternatives are selectable: none, cursory, partial, or total**.**

3.4.5. Accessibility factor. This section provides the selected accessibility factor and the rationale for selecting the factor. The accessibility factor relates the degree to which the operation, data, infrastructure, or system needs to be available from a security perspective. Here, availability concerns are those that relate to security risks, (i.e., non-tolerable operational impacts, and does not include those that are only performance concerns). Four alternatives are selectable: reasonable, soon, ASAP, or immediate**.**

3.4.6. Accuracy factor. This section should include the selected accuracy factor and the rational for selecting the factor. The accuracy factor relates the degree to which the integrity of operation, data, infrastructure, or system is needed from a security perspective. Here, integrity concerns are those that relate to security risks, (i.e., non-tolerable operational impacts, and does not include those that are only performance concerns). Three alternatives are selectable: non-applicable, approximate, or exact**.**

3.4.7. Information categories. This section should include the selected information categories and the rationale for selecting the categories. The mission of each system will determine the information processed. The mission and information will influence the environment and security requirements applicable to each information category. Information categories are defined by their relationships with common management principles and security requirements promulgated by the security policy for each information category. Processing, transmission, storage, and data of more than one category of information does not create a new category but instead inherits and must satisfy all the security requirements of the assigned categories. Each of the identified categories may carry additional restrictions or special handling conditions, (e.g., NATO-releasable or NOFORN). The information categories are as follows: Unclassified, Sensitive Information, Privacy Act, Financially Sensitive, Proprietary, Administrative/Other, Collateral Classified, Compartmented/Special Access Classified**.**

3.4.8. System class level. This section includes a completed system characteristic chart that provides the selected characteristics for the system and the rationale for selecting the alternative for the system. Exhibit 2 provides an example of a completed System Characteristic Chart.

Characteristic	**System**	**Alternatives**
Interfacing Mode	Active	Benign, Passive, or Active
Processing Mode	System High	Dedicated, Compartmented, System High, or Multilevel

Attribution Mode	Basic	None, Rudimentary, Selected, Basic, or Comprehensive
Mission-Reliance Factor	Partial	None, Cursory, Partial, or Total
Accessibility Factor	ASAP	Reasonable, Soon, ASAP, or Immediate
Accuracy Factor	Approximate	Not-applicable, Approximate, or Exact
Information Categories	Sensitive	Unclassified, Sensitive Information, Collateral Classified, or Compartmented/Special Access Classified

Exhibit 2: Completed System Characteristic Chart

3.4.9. Certification analysis level. This section should provide the certification level and a description of the certification requirements for the determined level. A chart for determining the certification level is provided in Enclosure 4 of this document. The completed certification level chart should be included in Appendix E of the SSAA. The certification level is used to scope the certification tasks to be performed in Phases 2 and 3 of the DITSCAP. The DITSCAP Implementation Guide, Section 3, C3.3.8 provides a description of each certification level.

3.5. System Security Requirements. The system security requirements are derived from the security policy. Examples of requirements are Identification and Authentication (I&A), contingency planning, access controls, etc. The security analysis levels stipulate the high-level security requirements. Include those required by directives, those due to connection with other networks and systems, those required by data originators, and any additional requirements specified by the DAA. Requirements of all ITSEC disciplines (COMPUSEC, COMSEC, TEMPEST, physical security, personnel security) must be included. A common approach to prepare this section is to construct a Requirements Traceability Matrix (RTM). The DITSCAP Implementation Guide, Section 3, table C3-7, provides an example of a RTM (The review column identifies the review process for each requirement, where I - Interview, D - Document review, T - Test, and O - Observation.). The RTM should be included as Appendix F to the SSAA. An example RTM is provided in Enclosure 3.

3.5.1. Federal and DoD Security Requirements. This section provides a general description of the Federal and DoD automated information system security requirements. Enclosure 3 provides the basic security requirements for DoD systems processing Privacy Act information.

3.5.2. Governing Security Requisites. This section identifies all applicable Federal and DoD requirement documents.

3.5.3. Data Security Requirements. This section identifies and specifies all applicable security requirements specific to the system data.

3.5.4. Security CONOPS. This section provides the security concept of operations, which provides a detailed description of system input, system processing, and intermittent and final outputs. Descriptions of

all interactions and connections with external systems must be included. Use of diagrams, maps, pictures, and tables are encouraged. This section must be understandable by non-technical personnel.

3.5.5. Network Connections rules. This section provides a general overview of the policies regarding network or system connections to the system described in the SSAA.

3.5.5.1. Rules to connect to this system. This section (if applicable) provides the specific policies and procedures organizations must follow to connect networks or system to the system described in the SSAA.

3.5.5.2. Rules to connect to the other systems defined in the CONOPS. This section (if applicable) provides specific policies and procedures for connection to other systems defined in the CONOPS section of the SSAA.

3.5.6. Configuration and change management requirements. This section should provide a brief description of the change management control or configuration control procedures. Detailed information should be provided in Appendix O to the SSAA. The appendix should provide a brief description of the functional and physical characteristics of the system, the policies for controlling changes to those characteristics, and the policies for recording and reporting changes to the system.

3.5.7. Reaccreditation requirements. This section provides the requirements for the reaccreditation of the system. Systems are normally accredited for three years or until major system changes are implemented, at which time the system must be reaccredited.

3.5.8. Security Policy. The C&A team may chose to add the security policy in this section or add it in an additional appendix. In general terms, this section provides what is and is not permitted in the field of security during the general operation of the system. The security policy section describes the exceptions to the policies contained in the laws, regulations, rules, and practices that regulate how an organization manages, protects, and distributes information. This section establishes policy precedence when more than one policy applies. A list of polices that apply to the system is provided. The primary thrust of this section is to develop mission-level security objectives through deductive reasoning. Security objectives are the top-most level of specifications and focus on the security related aspects of the identified mission. Security objectives must be concise, declarative sentences derived from analysis of mission information, threat, and umbrella security guidance. These security objectives should be written in terms independent of architecture and implementation. Each security objective should be justified by rationale. The rationale documents the mission objectives supported by that security objective, the threat driving the security objective, the consequences of not implementing the objective, and applicable umbrella security guidance supporting that security objective. The rationale binds each security objective to a mission objective and focuses attention on security at the mission level.

3.6. Organizations and Resources. This section provides a statement indicating that the identified organizations are responsible for ensuring compliance with the SSAA. The DITSCAP Implementation Guide, Section 3, C3.3.7, provides additional guidance on the preparation of this section.

3.6.1. Identification of Organizations. This section describes the organization responsible for ensuring compliance with the SSAA and in the subsections, identify all of the participants, including the DAA, CA, user representative, Information System Security Officer (ISSO), and any other responsible organization offices that may be needed to support the C&A effort.

3.6.1.1. DAA. This section identifies the approving DAA. Provide the DAA's name, title, office and contact information (telephone number).

3.6.1.2. Certification Authority. This section should identify the Certification Authority. Provide the CA's name, title, office, and telephone number.

3.6.1.3. User Representative. This section identifies the User Representative. Provide the User Representative's name, title, office, and telephone number.

3.6.1.4. Responsible Organization and ISSO. This section identifies the organization responsible for the system and the ISSO. Provide the organizations official title and the ISSO's name, title, office and, contact information telephone number.

3.6.1.5. Program Manager and other organization offices. This section identifies the system Program or System Manager and any other responsible organization offices that may be needed to support the C&A effort. Provide the Program Manager's name, title, office, and telephone number. Provide the title of any other responsible organization offices needed to support the C&A effort (e.g. Configuration Management, Acquisition, Maintenance, and Administration).

3.6.2. Resources. This section provides a brief description of the personnel staffing and funding requirements to support the C&A process. Detailed information should be provided in the subsections. The CA may obtain assistance from a contractor team or other government organizations to analyze the system. The composition and size of the team should depend upon the size and complexity of the system under examination. The team shall have composite expertise in activities required, and who are independent of the system developer or Program Management.

3.6.2.1. Staffing requirements. This section identifies the C&A team staffing requirements for completion of the C&A process.

3.6.2.2. Funding requirements. This section identifies the C&A funding requirements for completion of the C&A process.

3.6.3. Training for the Certification Team. This section describes the training requirements, (types of training, who is responsible for preparing and conducting the training, equipment that will be required to conduct training, and training devices) of the certification team.

3.6.4. Roles and Responsibilities. This section provides a brief statement identifying the major participants in the C&A process, including the DAA, CA, User Representative, ISSO, and any other organizations that may be needed to support the C&A effort. The section should include information regarding each participant's responsibility for complying with the assigned roles and responsibilities. General roles and responsibilities of each major participant are further described in each subsection.

3.6.4.1. DAA. This section describes or lists the general responsibilities of the DAA. The DITSCAP Implementation Guide sections (as provided below) provide examples of the detailed responsibilities of the DAA during each phase of the DITSCAP.

• Table C3-12	DITSCAP Phase 1
• Section C4.4.1.1	DITSCAP Phase 2
• Table C5-4	DITSCAP Phase 3
• Table C6-6	DITSCAP Phase 4

3.6.4.2. Certification Authority. This section describes or lists the general responsibilities of the Certification Authority. The DITSCAP Implementation Guide sections (as provided below) provide examples of the detailed responsibilities of the DAA during each phase of the DITSCAP.

• Table C3-15	DITSCAP Phase 1
• Table C4-6	DITSCAP Phase 2
• Table C5-5	DITSCAP Phase 3
• Section C6.4.1.2	DITSCAP Phase 4

3.6.4.3. User Representative. This section describes or lists the general responsibilities of the User Representative. The DITSCAP Implementation Guide sections (as provided below) provide examples of the detailed responsibilities of the User Representative during each phase of the DITSCAP.

• Table C3-15	DITSCAP Phase 1
• Table C4-8	DITSCAP Phase 2
• Table C5-7	DITSCAP Phase 3
• Table C6-7	DITSCAP Phase 4

3.6.4.4. ISSO. This section describes or lists the general responsibilities of the ISSO. The DITSCAP Implementation Guide sections (as provided below) provide examples of the detailed responsibilities of the ISSO during each phase of the DITSCAP.

• Table C3-14	DITSCAP Phase 1
• Table C4-7	DITSCAP Phase 2

Table C5-6	DITSCAP Phase 3
Table C6-8	DITSCAP Phase 4

3.6.4.5. Additional Organizations. This section identifies and describes, or lists the general responsibilities of the other offices within the responsible organization needed to support the C&A process. The DITSCAP Implementation Guide sections (as provided below) provide examples of the detailed responsibilities of the additional organizations needed to support the C&A process.

Section C3.4.3-C3.4.3.5	DITSCAP Phase 1
Section C4.4.3-C4.4.3.5	DITSCAP Phase 2
Section C5.4.3-C5.4.3.2	DITSCAP Phase 3
Section C6.4.3-C6.4.3.5	DITSCAP Phase 4

3.6.5. Additional Supporting Organizations or Working Groups. This section identifies any additional organizations or working groups needed to support the C&A process. Provide the organization's title and the point of contact name.

3.7. Appendices.

A. Acronym List. This appendix lists and defines all acronyms used within the SSAA.

B. Definitions. This appendix lists and defines all terms used within the SSAA that may not be common knowledge to most users of the SSAA.

C. References. This appendix lists all applicable references.

D. DITSCAP Plan. This appendix documents the tailoring of the C&A process and defines a plan for accomplishing the required C&A tasks. Proper scheduling and subsequent agreement on the schedule will help ensure proper documentation is prepared and available for the C&A team review. The tasks, milestones, and schedule shall be defined in such a manner as to be consistent with the system development or maintenance schedule. The level of effort, roles and responsibilities shall also be consistent with the program development process and management plan. The DITSCAP Plan provides the vehicle to develop a mutual understanding of the system among organizations. The DITSCAP Implementation Guide, Sections 3, C3.3.8, Sections 7 and 8, provide some additional information for preparing this section. A suggested outline for the DITSCAP Plan is provided in DoD 5200.40 (DITSCAP), Enclosure 3.

E. Certification Level Determination. This appendix provides the completed Certification Level Determination Chart. An example of a Certification Level Determination Chart is provided in Enclosure 4 of this document.

F. Security Requirements or RTM. This appendix provides the system security requirements as derived from the security policy. Examples of requirements are I&A, contingency planning, access controls, etc. Include security requirements required by directives, those due to connection with other networks and systems, those required by data originators, and any additional requirements specified by the DAA. Requirements of all ITSEC disciplines (COMPUSEC, COMSEC, TEMPEST, physical security, personnel security) must be included. A common approach to prepare this section is to construct a Requirements Traceability Matrix (RTM). The DITSCAP Implementation Guide, Section 3, Table C3-7, provides an example of a RTM (The review column identifies the review process for each requirement, where I - Interview, D - Document review, T - Test, and O – Observation). An example RTM providing the basic Federal and DoD security requirements for systems processing Privacy Act information is provided in Enclosure 3.

G. System Architecture. This appendix provides the framework for the information system architecture and includes a physical description of the hardware, software, firmware, and interfaces. Against this framework, the architecture description stipulates the security architecture. Existing or planned system

features that facilitate expansion or external connection should be mentioned in this section. During the concept development phase, the architecture may not be fully developed. A broad description of these areas may be provided. However, once the information system has entered the design phase, the architecture description must be updated and details filled in. Areas may exist that do not apply to the information system (e.g., firmware). For such an instance, it is appropriate to enter the term "nonapplicable." Adequate detail should be included to compare the system's architecture with the Technical Architecture Framework for Information Management (TAFIM) Volume 6, Defense Goal Security Architecture (DGSA). Detailed information for all subsections of Section 3 of the SSAA should be included. The DITSCAP Implementation Guide, Section 3, C3.3.4, provides additional information for completing this section.

H. Security Test and Evaluation Plan, Procedures, and Results. This appendix describes both the expected and actual test outcomes for the security mechanisms or features, at both the system and application level. All security features must be tested at both the system and application level; this includes the C2 requirements of Audit, Discretionary Access Control, and Identification and Authentication, and object reuse. Test documentation describes the test plan, test logs, test reports, test procedures, and test results and explains how the security mechanisms were functionally tested.

I. System Rules of Behavior. This appendix provides an established set of rules of behavior concerning use of, security in, and the acceptable level of risk for, the system. The rules shall be based on the needs of the various users of the system. The security required by the rules shall be only as stringent as necessary to provide adequate security for information in the system. Such rules shall clearly delineate responsibilities and expected behavior of all individuals with access to the system. They shall include appropriate limits on interconnections to other systems and shall define service provision and restoration priorities. Finally, they shall be clear about the consequences of behavior not consistent with the rules.

J. Contingency Plan(s). This appendix contains the plan for the rapid recovery of a system in the event of an outage or interruption to automated mission operations. This document should describe the emergency responses, backup procedures, backup operations, recovery, and emergency destruction of classified data. An outage or interruption may be caused by damage to facilities, equipment, software, or data that comprise the system or application. The plan provides an organized method for restoring automated mission operations to a useable level that will support crucial mission functions during times of emergency or until full and permanent operations can be restored. The plan defines the responsibilities of each person expected to play a role during the emergency and requirements for testing the plan. The detail of the contingency plan is influenced by the IT environment, the criticality of the functional applications being supported, and the user's requirements.

K. Security Awareness and Training Plan. This appendix contains the security training plan and documentation based on the written rules of the system. The type of training and the content should be specific to what each type of user needs to know to use the system securely. Documentation should include how specific groups of users will be trained and what that training will include. Subjects to be covered should include work at home, dial-in access, connection to the Internet, use of copyrighted works, unofficial use of government equipment, the assignment and limitation of system privileges, individual accountability, technical security controls (e.g., password use), proper use of applications, how to get help, and restoration of service as a concern of all users of the system or application.

L. Personnel Security Controls. This appendix provides a statement indicating the responsible organization complies with the appropriate personnel security requirements. An example statement is provided in Enclosure 5.

M. Incident Response Plan. This appendix provides policies and procedure for providing a capability to help users when a security incident occurs in the system and to share information concerning common vulnerabilities and threats. This capability should assist the organization in pursuing appropriate legal action if necessary. The appendix should address reporting requirements for security incidents and actions to be taken.

N. Memoranda of Agreement/System Interconnect Agreements. This appendix contains all required memoranda of agreement (MOA). When systems managed by different DAAs are interfaced or networked, a MOA is required that addresses the accreditation requirements for each system involved. The MOA should include description and classification of the data, clearance levels of the users, designation of the DAA who shall resolve conflicts among the DAAs, and safeguards to be implemented before interfacing the systems. MOAs are required when one DoD component's system interfaces with another system within the same DoD component or in another DoD component and when a contractor's system interfaces with a DoD component's system or to another contractor's system.

O. Applicable System/Security Documentation. This appendix contains a list of appropriate system development or security documentation as developed. The appendix specifies the availability, source of the documentation, or a copy of the documentation.

Configuration Management Plan. **The change management control or configuration control procedures should be included. These procedures should identify and document the functional and physical characteristics of the system, control changes to those characteristics, and record and report change processing and implementation status.**

Security Features Users Guide. **Provide documentation describing the protection mechanisms provided by the system, guidelines on their use, and how they interact with one another.**

Trusted Facility Manual. **Provide documentation presenting the cautions about functions and privileges needing to be controlled when running a secure facility, as well as procedures for examining and maintaining audit files. Provide a detailed audit record structure for each type of audit event.**

Other System Documentation. **Provide the availability, source of the documentation, or a copy of the documentation.**

P. System Security Plan. Provide documentation indicating the agency's policies and procedures, management controls, operational controls, and technical controls. The National Institute of Standards and Technology (NIST) Special Publication 800-18 "*Guide for Developing Security Plans for Information Technology Systems*" should be used for developing the System Security Plan.

Q. Risk Assessment Results. This appendix includes an analysis of system assets and vulnerabilities to establish an expected loss from certain events based upon estimated probabilities of occurrence.

R. Certifying Authority's Recommendation and Documentation. This appendix contains the Statement of Certification, which provides the CA's recommendations for enhancing the security profile of the system, interim certification requirements, the length of certification time for the system, and other supporting documentation.

S. Accreditation Decision and Statement. This appendix contains the authorization to operate the system in a formal memorandum (Accreditation Statement) from the DAA to the acquisition agency.

Enclosure 1
Acronym List

Acronym	Definition
AIS.......................	**Automated Information System**
C&A	**Certification and Accreditation**
CA........................	**Certifying Authority**
COMPUSEC	**Computer Security**
COMSEC	**Communications Security**
CONOPS	**Concept of Operations**
COTS	**Commercial Off-the-Shelf**
DAA.....................	**Designated Approving Authority**
DGSA	**Defense Goal Security Architecture**
DITSCAP	**Defense Information Technology Security Certification and Accreditation Process**
DoD......................	**Department of Defense**
EPL...................... **............................**	**Evaluated Products List**

EPROM...............	**Enhanced PROM**
GOTS	**Government Off-the-Shelf**
IAW.....................	**In Accordance With**
ISSO	**Information System Security Officer**
ITSEC..................	**Information Technology Security**

MOA.................... **............................**	**Memoranda of Agreement**
NATO..................	**North Atlantic Treaty Organization**
NIST	**National Institute of Standards and Technology**
NOFORN	**No Foreign**
NSA	**National Security Agency**
PROM	**Programmable Read-Only Memory**
RTM	**Requirements Traceability Matrix**
SFUG...................	**Security Features Users Guide**
SSAA	**System Security Authorization Agreement**
SSP.......................	**System Security Plan**
TAFIM	**Technical Architecture Framework for Information Management**
TFM.....................	**Trusted Facility Manual**

Enclosure 2

Suggested SSAA Outline

The following outline is recommended for use for preparing a SSAA. At a minimum, the SSAA should contain the information provided below.

1. MISSION DESCRIPTION AND SYSTEM IDENTIFICATION

1.1. System name and identification
1.2. System description
1.3. Functional description
1.3.1. System capabilities
1.3.2. System criticality
1.3.3. Classification and sensitivity of data processed
1.3.4. System user description and clearance levels
1.3.5. Life cycle of the system
1.4. System CONOPS summary

2. ENVIRONMENT DESCRIPTION

2.1. Operating environment
2.2. Software development and maintenance environment
2.3. Threat description

3. SYSTEM ARCHITECTURAL DESCRIPTION

3.1. Hardware
3.2. Software
3.3. Firmware
3.4. System interfaces and external connections
3.5. Data flow
3.6. DGSA Security View
3.7. Accreditation boundary

4. ITSEC SYSTEM CLASS

4.1. Interfacing mode
4.2. Processing mode
4.3. Attribution mode
4.4. Mission-reliance factor
4.5. Accessibility factor
4.6. Accuracy factor
4.7. Information categories
4.8. System class level
4.9. Certification analysis level

5. SYSTEM SECURITY REQUIREMENTS

5.1. National/DoD security requirements
5.2. Governing security requisites
5.3. Data security requirements
5.4. Security CONOPS
5.5. Network connection rules
5.5.1. To connect to this system
5.5.2. To connect to the other systems defined in the CONOPS
5.6. Configuration and change management requirements
5.7. Reaccreditation requirements

6. ORGANIZATIONS AND RESOURCES

6.1. Identification of organizations
6.1.1. Designated Approving Authority (DAA)
6.1.2. Certification Authority (CA)
6.1.3. Identification of the User Representative
6.1.4. Identification of the organization responsible for the system
6.1.5. Identification of the Program Manager or System Manager
6.2. Resources
6.2.1. Staffing requirements
6.2.2. Funding requirements
6.3. Training for certification team
6.4. Roles and responsibilities
6.5. Other supporting organizations or working groups

APPENDICES:

APPENDIX A Acronym List
APPENDIX B Definitions
APPENDIX C References
APPENDIX D DITSCAP Plan
APPENDIX E Certification Level Determination
APPENDIX F Security Requirements and/or Requirements Traceability Matrix
APPENDIX G System Architecture
APPENDIX H Security Test and Evaluation Plan, Procedures, and Results
APPENDIX I System Rules of Behavior
APPENDIX J Contingency Plan(s)
APPENDIX K Security Awareness and Training Plan
APPENDIX L Personnel Security Controls
APPENDIX M Incident Response Plan
APPENDIX N Memoranda of Agreement - System Interface Agreements
APPENDIX O Applicable System/Security Documentation (CMP, TFM, SFUG)
APPENDIX P System Security Plan (SSP)
APPENDIX Q Risk Assessment Results
APPENDIX R Certifying Authority's Recommendation and Documentation
APPENDIX S Accreditation Statement

Enclosure 4

Certification Level Chart

Characteristic	System Selection	Selection Values	Assigned Weight
Interfacing Mode		Benign (w=1) Passive (w=3) Active (w=7)	
Processing Mode		Dedicated (w=1) Compartmented (w=2) System High (w=5) Multi-level (w=8)	
Attribution Mode		None (w=1) Rudimentary (w=2) Selected (w=4) Comprehensive (w=6)	
Mission-Reliance Factor		None (w=0) Cursory (w=1) Partial (w=3) Total (w-7)	
Accessibility Factor		Reasonable (w=1) Soon (w=2) ASAP (w=4) Immediate (w-7)	
Accuracy Factor		Non-Applicable (w=0) Approximate (w=2) Exact (w=5)	
Information Categories		Unclassified (w=0) Sensitive (w=2) Collateral (w=5) Compartmented (w=7)	
System Weight Total			

Certification Level	Total System Weight Score Levels
Level 1	Conduct a Level 1 certification if the System Weight Score is **<17**
Level 2	Conduct a Level 2 certification if the System Weight Score is =**17** < **26**
Level 3	Conduct a Level 3 certification if the System Weight Score is =**20** < **37**
Level 4	Conduct a Level 4 certification if the System Weight Score is =**30**

Enclosure 5

ADP Position Designation Letter (Example)

MEMORANDUM FOR CHIEF, MILITARY HEALTH SYSTEM AUTOMATED
INFORMATION SYSTEMS SECURITY PROGRAM

SUBJECT: Automated Data Processing (ADP) Position Sensitivity Designations

As the Program Manager for ***(network or application*)**, I certify that a Personnel Security Program for **(*network or application)*** is in place IAW DoD 5200.2-R and the MHS AIS Security Policy Manual. Each person assigned to a position designated as level ADP-I, ADP-II, or ADP-III has completed the appropriate forms.

Signature Block

Information Management, Technology, and Reengineering

Attachment 4

HEALTH AFFAIRS

Military Health System (MHS) Information Assurance (IA) Risk Assessment Report FOR FULL SYSTEM NAME (ACRONYM)

Date [Month Year]

MASTER TEMPLATE

Prepared for:
Military Health System (MHS)
Information Assurance (IA) Program Office

Table of Contents

List of Tables

LIST OF FIGURES

Instructions: Update TOC to include applicable figures and diagrams.

Appendices

INTRODUCTION

Purpose

Instructions: Select the Background paragraph based on the XYZ System risk analysis scenario.

A Risk Assessment for the *XYZ System* Full System Name (Acronym) was performed to ascertain the extent to which it meets the Department of Defense (DoD) C2 security requirements in order to obtain an Interim Approval to Operate (IATO). These requirements are set forth in DoD 5200.28-STD, "DoD Trusted Computer System Evaluation Criteria," dated, December 1985. Appendix A provides a listing of the requirements set forth by the aforementioned reference. This report reviews the security requirements for the *XYZ System*, summarizes key security activities supporting certification and accreditation (C&A), and identifies recommendations regarding an IATO.

Select one of the following:

New system never certified or accredited: The *XYZ System* is a new AIS in development which is being deployed prior to completion of a full Authority To Operate (ATO) can be completed. Therefore an IATO is being considered for issuance for period up to 12 months.

ATO is about to expire: The *XYZ System* has a current ATO about to expire and has not completed the ATO before the current ATO expires, an IATO may be issued. The IATO is based on the findings from the previous annual report and findings. Therefore an IATO is being considered for issuance for period up to 12 months.
AIS pending migration or deletion: The *XYZ System* needs to maintain its ATO pending a replacement AIS or migration into another system that is not deployed. This IATO is based on the findings from the previous annual report and findings. Therefore an IATO is being considered for issuance for period up to 12 months.
AIS undergoing a major change: The *XYZ System* is undergoing a major system change and needs an IATO to continue its current ATO while the system changes are completed. The IATO is based on the findings from the previous annual report and findings Therefore an IATO is being considered for issuance for period up to 12 months. A full ATO will be conducted when the major changes are completed.

The *XYZ System* is a mission critical system (or network) and is currently operational. The network was previously accredited at the DoD C2 level of trust. The system (or network) is being considered for an IATO to allow adequate time to complete the full certification and accreditation process for issuance of a full Authority To Operate (ATO).

Scope

Identify security vulnerabilities and weaknesses in the *XYZ System* located at [**Instructions:** State address of where testing was performed] 111 Market Place, Baltimore, Maryland by performing Security Test and Evaluation (ST&E) activities. Additional requirements for the *XYZ System* ST&E included:

- DoD Regulation 5400.11, “DoD Privacy Act Program,” dated June 1982

LIMITATIONS

The risk assessment is a preliminary evaluation of the automated information system (AIS) or network to uncover potential threats[1], vulnerabilities[2], and points of failure that can affect the confidentiality, integrity, and availability of the system or network. The activity considers major factors in risk management, the value of the system or application, threat, vulnerabilities, and the effectiveness of the proposed safeguards. This risk assessment is an interim measure within the MHS certification and accreditation process to ascertain the security threats and vulnerabilities of an AIS in advance of a full Approval to Operate (ATO) in order to achieve key project milestones or continued sustainment.

responsibility matrix

Name	Title	Responsibility
Lt. Col. HGFD	Designated Approving Authority (DAA)	Official responsible for accepting the level of risk for MHS Managed Care Support Contractors (MCSC), including *XYZ System*; grants accreditation or IATO

[1] A threat is defined as any circumstance or event with the potential to cause harm to an AIS through unauthorized access, destruction, disclosure, modification of data, and/or denial of service.

[2] A vulnerability is defined as any weakness in an AIS, system security procedure, internal controls, or implementation that could be exploited.

Mr. ABCS	XYZ System Information Systems Security Officer (ISSO)	OFFICIAL WITH THE AUTHORITY TO FORMALLY ASSUME RESPONSIBILITY FOR OPERATING THE AIS AT AN ACCEPTABLE RISK; GRANTS ACCREDITATION OR IATO.
Ms ASDF	Certification Authority (CA)	Responsible for making a technical judgment of the system's compliance with stated requirements, identify and assess risks associated with operating the AIS, coordinating the certification activities, and consolidating the supporting certification documentation.
Ms. ABC [Identify Name of Analyst. If a scan was performed, identified security engineer as well.]	Security IA Analyst(s)	Perform activities identified in this report, such as: • Requirements Analysis • Documentation Review • Risk Analysis/Review • Security Testing

Table 1: XYZ System Risk Assessment Responsibility Matrix

aSSUMPTIONS

The following assumptions were made during this risk assessment:

- If the system (or network) does not meet the requirements stated in the System Security Authorization Agreement (SSAA), but mission criticality mandates that the system become/remain operational, an IATO may be issued at the direction of the DAA. The MHS DAA, MHS CA, and user representative will determine the proposed solutions, schedule, security actions, milestones, and maximum length of time for the IATO validity.
- *XYZ System* personnel will address all the security parameters identified in the SSAA and resolve security deficiencies identified in this report within the time period identified to achieve an ATO.
- *XYZ System* personnel will comply with all applicable established DoD security policies, standards and guidelines throughout the network development lifecycle.
- *XYZ System* personnel will perform mandatory security training for the Information System Security Officer, network and system administrators, and users as identified in the system security training plans.
- *XYZ System* will operate in a secured environment in accordance with site operational and environmental procedures to ensure that risk to confidentiality, integrity, availability, and accountability of the information and network remains acceptable.

Documentation responsibilities

The MHS IA Program Office has tasked Federal Technology Corporation (Fed Tec) with development of the AIS Risk Assessment report for *XYZ System* (under Delivery Order 47, Deliverable 10). This document contains a summary of the security testing results to validate the security controls currently implemented;

provides identified vulnerabilities for those that have countermeasures; and, identifies which vulnerabilities that do not have appropriate security controls.

The FedTec team has a composite level of experience equivalent to 50 year in the areas of Information Management Technology & Reengineering, Military Health Systems AISs, system development, testing, system and security engineering, and information assurance, including specific proficiency with the DoD Information Technology Security Certification and Accreditation Process (DITSCAP) supporting the MHS IA program.

Document Organization

This report describes the risk assessment activities for the *XYZ System* and is organized as follows:

- Section 1 provides the purpose and scope of the Risk Assessment. It also identifies the scope and accreditation boundary, and the roles and responsibilities of key participants in the Risk Assessment process.
- Section 2 details the *XYZ System* architecture including identification of the system capabilities and technical components.
- Section 3 identifies the technical criteria and evaluation activities utilized during the risk assessment.
- Section 4 documents the detailed findings and recommendations that resulted from the risk assessment.
- Section 5 summarizes the risk assessment findings and presents the evaluation determination.
- Appendix A identifies the Security Requirements and related security reference documentation.
- Appendix B provides the standard MHS security definition of technical terms.
- Appendix C describes the *XYZ System* Test Plan.
- Appendix D lists the tests that were performed and the results of those tests.

System OVERVIEW

System Background

[**Instructions**: *Completeness of this section is contingent on the availability of system documentation.* Provide a brief summary of the system. Include: AIS Name, responsible organization, AIS Category (e.g., mission critical, mission support), operational status (development phase), general description and purpose (scope/objective of the system), interfaces, etc.]

> The *XYZ System* is responsible for all aspects of automated information systems (AIS) security as they apply to the MHS managed care support contract in Region 1 of the TRICARE Program. All AIS Security Policies are in compliance with Federal, State, and Local laws, DoD Directives, and the corporate AIS Security Policies of Sierra Health Services, Inc.

The *XYZ System* is in phase four of the Life Cycle Management, "operation and support." Because of the sensitivity of the data processed, the *XYZ System* is categorized as sensitive unclassified in accordance with criteria established by the Computer Security Act of 1987. The data is protected under the Privacy Act of 1974 and the Health Insurance Portability and Accountability Act (HIPAA) of 1996. The XYZ System was previously approved to operate at the C2 Level of Trust and still currently operates in the "System High" mode of operation.

1. *Major Functional Capabilities*

[**Instructions:** Identify the major functions of the system (e.g., order management, resource allocation management, results reporting.]

The XYZ System provides network connectivity and supporting administrative services to members of the XYZ System staff and partner providers. The user devices and partner provider applications are interconnected.

2. *Interfaces*

[**Instructions:** Identify MHS AIS interfaces]. In addition, the *XYZ System* interfaces with external systems including [**Instructions:** Identify external system interfaces (e.g., DEERS)].

The XYZ System is a stand-alone general support system with connectivity to the Composite Health Care System (CHCS), Defense Eligibility Enrollment Reporting System (DEERS), Sierra Health Services (SHS), Blue Cross/Blue Shield of South Carolina (BCBSSC), and the untrusted public domain (Internet).

3. *XYZ System Architecture*

The *XYZ System* employs a system architecture and data storage and recovery technologies designed to meet data availability and integrity requirements such as system redundancy (elimination of single points of failure), disk shadowing, mirroring, redundant array of inexpensive disk (RAID) technology, and operational processes (e.g., journaling) to minimize data loss. An approved off-site storage facility is utilized to maintain copies of archived data that serves as a backup source in the event of a catastrophic loss of information resources.

For the purpose of this requirement, data loss is defined as the unrecoverable loss of clinical health care or administrative information resulting from deletion, corruption, loss of integrity, loss of synchronization, or unauthorized modification, making the information unavailable to XYZ System or the Government.

FIGURE 1 ILLUSTRATES THE *XYZ SYSTEM* WIDE AREA NETWORK (WAN):

[**Instructions:** Insert Logical Diagrams of the XYZ System – should be provided by the XYZ System developers. Update TOC.]

Figure 1: *XYZ System* Wide Area Network

Figure 2 illustrates the *XYZ System* Remote Access infrastructure:

Figure 2: *XYZ System* Remote Access Infrastructure

Figure 3 illustrates the *XYZ System* Private Intranet (i.e., private network):

Figure 3: *XYZ System* Private Intranet

Software

[**Instructions:** Identify the software components that comprise the XYZ System. Note which products are COTS vs. GOTs.]

The *XYZ System* uses software applications that are configured for Windows 95 and uses Windows NT to manage data, files, and applications. The application software includes the following:

- Microsoft Windows NT Server 4.0
- Microsoft Structured Query Language (SQL) 6.5
- Microsoft SMS 1.2 for Systems Management
- Microsoft Office for Windows 95 workstations
- Rumba for Windows 95 workstations (for telnet sessions)
- Microsoft Exchange 5.0
- Microsoft Internet Explorer

Hardware

[**Instructions:** Identify the hardware components that comprise the XYZ System – configuration. Identify if the test configuration is the same as the proposed operational configuration.]

The hardware configuration for the *XYZ System* is based on the Digital Equipment Corporation (DEC) Alpha servers product line and Intel Pentium Personal Computers, along with the Microsoft Windows NT operating system. Cisco routers provide connectivity using the cryptography feature in the software. Each configuration includes a disk drive for system files and separate directories adequate for long-term database needs.

SECURITY Test and Evaluation

Technical Criteria and approAch

The MHS Risk Assessment process is designed to determine the extent to which an AIS meets the minimum DoD C2 technical requirements as defined in DoD 5200.28-STD, "DoD Trusted Computer System Evaluation Criteria," dated, December 1985, as identified in Appendix A.

[**Instructions:** Identify the boundaries of the risk assessment.]

This risk assessment was limited to the network directly supporting the MHS TRICARE mission. Testing and analysis was limited to the basic configuration of the XYZ System Windows NT 4.0 Servers that process TRICARE Medical Activity (TMA) data and the extent to which the security mechanisms satisfy the minimum DoD C2 requirements listed in Appendix A.

The *XYZ System* Test Plan can be found in Appendix C. The specific tests that were conducted, as well as the results of those tests can be found in Appendix D.
Additional requirements that were considered for the *XYZ System* Security Testing and Evaluation included:

- DoD Regulation 5400.11, "DoD Privacy Act Program," dated June 1982

The *XYZ System* risk assessment activities included:

- Security Test and Evaluation. Test procedures were provided by the XYZ System representatives; compared and executed against the Minimum C2 Checklist (Appendix A) and reported to XYZ System management for remediation.
- Documentation Review: Available system and security documentation was provided for information and evaluation. The documentation was reviewed for quality and completeness based on the requirements set forth in the DITSCAP guidance and MHS-provided templates.

Note: An automated vulnerability scan was not performed as part of this risk assessment. A system scan will be conducted as part of the full ATO process.

Evaluation activities

Evaluation activities for *XYZ System* operational environment included Security Testing on December 19, 2001 at 111 Market Place, Baltimore, Maryland. A review of MHS-required documentation, as well as additional documentation was conducted. Interviews with *XYZ System* support personnel were also conducted during test activities.

MHS-required documentation included:

- Draft Core SSAA
- Draft Security Network Design Documentation
- Test Procedures

Additional *XYZ System* security documentation included:

- *XYZ System* Information Systems Division Information Security Policy and Standard Operating Procedures
- *XYZ System* Information Systems Division Security Features Users Guide
- *XYZ System* Continuity Of Operations Plan (COOP)
- *XYZ System* Information Systems Division Systems Security Plan
- *XYZ System* Trusted Facility Manual
- *XYZ System* TRICARE Service Center System Operations Manual (TSCSOM)

EVALUATION RESULTS

Risk Assessment Vulnerabilities

Discretionary Access Control (DAC)

Requirement

The Trusted Computing Base (TCB) shall define and control access between named users and named objects (e.g., files and programs) in the ADP system. The enforcement mechanism (e.g., self/group/public controls, access control lists) shall allow users to specify and control sharing of those objects by named individuals, or defined groups of individuals, or by both, and shall provide controls to limit propagation of access rights. The discretionary access control mechanism shall, either by explicit user action or by default, provide that objects are protected from unauthorized access. These access controls shall be capable of including or excluding access to the granularity of a single user. Access permission to an object by users not already possessing access permission shall only be assigned by authorized users.

Assessment Findings

*[**Instructions:** List all DAC Findings and Recommendations separately; number by section (1,2,3…). If no findings, state: "The evaluation has determined that the requirement for Discretionary Access Control is satisfied."]*

1. **Finding**: [**Instructions**: Enter DAC finding here.]

   Recommendation: [**Instructions:** Enter the MHS IA Recommendation (for a fix) here.]

   Current Status: [**Instructions:** Enter the status of the DAC finding here.]

   ***XYZ System* Response:** [**Instructions:** Include the program/project office response - if available.]

   Risk Rating: [**Instructions:** State "Low", "Medium", or "High" based on assessment.]

2. **Finding:**

   Recommendation:

   Current Status:

   ***XYZ System* Response:**

Risk Rating:

Object Reuse

1) Requirement

All authorizations to the information contained within a storage object shall be revoked prior to initial assignment, allocation or reallocation to a subject from the TCB's pool of unused storage objects. No information, including encrypted representations of information, produced by a prior subject's actions is to be available to any subject that obtains access to an object that has been released back to the system.

Assessment Findings

[**Instructions:** *List all Object Reuse Findings and Recommendations separately; number by section (1,2,3…). If no findings, state: "The evaluation has determined that the requirement for Object Reuse is satisfied."]*

1. Finding: [**Instructions:** Enter Object Reuse finding here.]

Recommendation: [**Instructions:** Enter the MHS IA Recommendation (for a fix) here.]

Current Status: [**Instructions:** Enter the status of the Object Reuse finding here.]

***XYZ System* Response:** [**Instructions:** Include the program/project office response - if available.]

Risk Rating: [**Instructions:** State "Low", "Medium", or "High" based on assessment.]

2. Finding:

Recommendation:

Current Status:

***XYZ System* Response:**

Risk Rating:

Identification and Authentication (I&A)

Requirement

The Trusted Computing Base (TCB) shall require users to identify themselves to it before beginning to perform any other actions that the TCB is expected to mediate. Furthermore, the TCB shall use a protected mechanism (e.g., passwords) to authenticate the user's identity. The TCB shall protect authentication data so that any unauthorized user cannot access it. The TCB shall be able to enforce individual accountability by providing the capability to uniquely identify each individual ADP system user. The TCB shall also provide the capability of associating this identity with all auditable actions taken by that individual.

Assessment Findings

[**Instructions:** *List all I&A Findings and Recommendations separately; number by section (1,2,3…). If no findings, state: "The evaluation has determined that the requirement for I&A is satisfied."]*

1. Finding: [**Instructions**: Enter I&A finding here.]

Recommendation: [**Instructions**: Enter the MHS IA Recommendation (for a fix) here.]

Current Status: [**Instructions**: Enter the status of the I&A finding here.]

XYZ System **Response:** [**Instructions:** Include the program/project office response - if available.]

Risk Rating: [**Instructions:** State "Low", "Medium", or "High" based on assessment.]

2. Finding:

Recommendation:

Current Status:

XYZ System **Response:**

Risk Rating:

Audit

Requirement.

The TCB shall be able to create, maintain, and protect from modification or unauthorized access or destruction an audit trail of accesses to the objects it protects. The audit data shall be protected by the TCB so that read access to it is limited to those who are authorized for audit data. The TCB shall be able to record the following types of events:

- Use of identification and authentication mechanisms
- Introduction or objects into a user's address space (e.g., file open, program initiation)
- Deletion of objects
- Actions taken by computer operators and system administrators and/or system security officers
- Any other security relevant events
- For each recorded event, the audit record shall identify:
  - Date and time of the event
  - User
  - Type of event
  - Success or failure of the event

For identification/authentication events the origin of request (e.g., terminal ID) shall be included in the audit record. For events that introduce an object into a user's address space and for object deletion events the audit record shall include the name of the object. The system administrator shall be able to selectively audit the actions of any one or more users based on individual identity.

Assessment Findings:

[**Instructions:** *List all Audit Findings and Recommendations separately; number by section (1,2,3…). If no findings, state: "The evaluation has determined that the requirement for Audit is satisfied."]*

1. **Finding**: [**Instructions:** Enter Audit finding here.]

   Recommendation: [Instructions: Enter the MHS IA Recommendation (for a fix) here.]

   Current Status: [**Instructions:** Enter the status of the Audit finding here.]

   ***XYZ System* Response**: [**Instructions:** Include the program/project office response - if available.]

   Risk Rating: [**Instructions:** State "Low", "Medium", or "High" based on assessment.]

2. **Finding:**

   Recommendation:

   Current Status:

   ***XYZ System* Response**:

   Risk Rating:

System Architecture

Requirement

The TCB shall maintain a domain for its own execution that protects it from external interference or tampering (e.g., by modification of its code or data structures). Resources controlled by the TCB may be a defined subset of the subjects and objects in the ADP system. The TCB shall isolate the resources to be protected so that they are subject to the access control and auditing requirements.

Assessment Finding

[**Instructions:** *List all Architecture Findings and Recommendations separately; number by section (1,2,3…). If no findings, state: "The evaluation has determined that the requirement for Architecture is satisfied."]*

1 **Finding**: [**Instructions:** Enter Architecture finding here.]

Recommendation: [**Instructions:** Enter the MHS IA Recommendation (for a fix) here.]

Current Status: [**Instructions:** Enter the status of the Architecture finding here.]

XYZ System **Response**: [**Instructions:** Include the program/project office response - if available.]

Risk Rating: [**Instructions:** State "Low", "Medium", or "High" based on assessment.]

2 Finding:

Recommendation:

Current Status:

XYZ System **Response:**

Risk Rating:

System Integrity

Requirement

Hardware and/or software features shall be provided that can be used to periodically validate the correct operation of the on-site hardware and firmware elements of the TCB.

Assessment Findings

[**Instructions:** *List all System Integrity Findings and Recommendations separately; number by section (1,2,3…). If no findings, state: "The evaluation has determined that the requirement for System Integrity is satisfied."]*

1. **Finding**: [**Instructions:** Enter System Integrity finding here.]

Recommendation: [**Instructions:** Enter the MHS IA Recommendation (for a fix) here.]

Current Status: [**Instructions:** Enter the status of the System Integrity finding here.]

XYZ System **Response**: [**Instructions:** Include the program/project office response - if available.]

Risk Rating: [**Instructions:** State "Low", "Medium", or "High" based on assessment.]

2. Finding:

Recommendation:

Current Status:

XYZ System **Response:**

Risk Rating:

Security Testing

Requirement

The security mechanisms of the ADP system shall be tested and found to work as claimed in the system documentation. Testing shall be done to assure that there are no obvious ways for an unauthorized user to bypass or otherwise defeat the security protection mechanisms of the TCB. Testing shall also include a search for obvious flaws that would allow violation of resource isolation, or that would permit unauthorized access to the audit or authentication data.

Assessment Findings

[**Instructions:** *List all Security Testing Findings and Recommendations separately; number by section (1,2,3…). If no findings, state: "The evaluation has determined that the requirement for Security Testing is satisfied."]*

1. Finding: [**Instructions:** Enter Security Testing finding here.]

Recommendation: [**Instructions:** Enter the MHS IA_Recommendation (for a fix) here.]

Current Status: [**Instructions:** Enter the status of the Security Testing finding here.]

***XYZ System* Response**: [**Instructions:** Include the program/project office response - if available.]

Risk Rating: [**Instructions:** State "Low", "Medium", or "High" based on assessment.]

2. Finding:

Recommendation:

Current Status:

***XYZ System* Response:**

Risk Rating:

b. Security Features User's Guide (SFUG)

Requirement

A single summary, chapter, or manual in user documentation shall describe the protection mechanisms provided by the TCB, guidelines on their use, and how they interact with one another.

Assessment Findings

[**Instructions:** *List all SFUG Findings and Recommendations separately; number by section (1,2,3…). If no findings, state: "The evaluation has determined that the requirement for SFUG is satisfied."]*

1. Finding: [**Instructions:** Enter SFUG finding here.]

Recommendation: [**Instructions:** Enter the MHS IA Recommendation (for a fix) here.]

Current Status: [**Instructions:** Enter the status of the SFUG finding here.]

XYZ System **Response**: [**Instructions:** Include the program/project office response - if available.]

Risk Rating: [**Instructions:** State "Low", "Medium", or "High" based on assessment.]

2. Finding:

Recommendation:

Current Status:

XYZ System **Response:**

Risk Rating:

c. Trusted Facility Manual (TFM)

Requirement

A manual addressed to the system administrator shall present cautions about functions and privileges that should be controlled when running a secure facility. The procedures for examining and maintaining the audit files as well as the detailed audit record structure for each type of audit event shall be given.

Assessment Findings

[**Instructions:** *List all TFM Findings and Recommendations separately; number by section (1,2,3…). If no findings, state: "The evaluation has determined that the requirement for TFM is satisfied."]*

1. Finding: [Instructions: Enter TFM finding here.]

Recommendation: [**Instructions:** Enter the MHS IA Recommendation (for a fix) here.]

Current Status: [**Instructions:** Enter the status of the TFM finding here.]

XYZ System **Response**: [**Instructions:** Include the program/project office response - if available.]

Risk Rating: [**Instructions:** State "Low", "Medium", or "High" based on assessment.]

2. Finding:

Recommendation:

Current Status:

***XYZ System* Response:**

Risk Rating:

d. Test Documentation

Requirement

The system developer shall provide to the evaluators a document that describes the test plan, test procedures that show how the security mechanisms were tested, and results of the security mechanisms' functional testing.

Assessment Findings

[**Instructions:** *List all Testing Documentation Findings and Recommendations separately; number by section (1,2,3…). If no findings, state: "The evaluation has determined that the requirement for Testing Documentation is satisfied."]*

- **Finding:** [**Instructions:** Enter Testing Documentation finding here.]

  Recommendation: [**Instructions:** Enter the MHS IA Recommendation (for a fix) here.]

  Current Status: [**Instructions:** Enter the status of the Testing Documentation finding here.]

  ***XYZ System* Response**: [**Instructions:** Include the program/project office response - if available.]

  Risk Rating: [**Instructions:** State "Low", "Medium", or "High" based on assessment.]

- **Finding:**

  Recommendation:

  Current Status:

  ***XYZ System* Response:**

  Risk Rating:

e. Security Design Documentation

Requirement

Documentation shall be available that provides a description of the manufacturer's philosophy of protection and an explanation of how this philosophy is translated into the TCB. If the TCB is composed of distinct modules, the interfaces between these modules shall be described.

Assessment Findings

[**Instructions:** *List all Security Design Documentation Findings and Recommendations separately; number by section (1,2,3…). If no findings, state: "The evaluation has determined that the requirement for Security Design Documentation is satisfied."]*

- **Finding:** [**Instructions:** Enter Security Design Documentation finding here.]

  Recommendation: [**Instructions:** Enter the MHS IA Recommendation (for a fix) here.]

  Current Status: [**Instructions:** Enter the status of the Security Design Documentation finding here.]

  ***XYZ System* Response**: [**Instructions:** Include the program/project office response - if available.]

  Risk Rating: [**Instructions:** State "Low", "Medium", or "High" based on assessment.]

- **Finding:**

  Recommendation:

  Current Status:

  ***XYZ System* Response:**

  Risk Rating:

Determination

RISK Assessment Summary

[**Instructions:** Summarize finding by key area; note the total number of finding/area; identify acceptance criteria.]
A total of three risk items are documented in this risk assessment. The following is a summary of the vulnerabilities identified during the assessment

- **Discretionary Access Control (DAC)** – no risks or exposures were noted during the assessment.
- **Object Reuse**– no risks or exposures were noted during the assessment.
- **Identification and Authentication (I&A)** – no risks or exposures were noted during the assessment.
- **Audit**– Two findings were noted. Both findings have a Low risk rating.
- **System Architecture** One finding was noted with a Low risk rating.
- **System Integrity** no risks or exposures were noted during the assessment.
- **Security Testing** – no risks or exposures were noted during the assessment.
- **Documentation)** – no risks or exposures were noted during the assessment.

The evaluation concluded that the *XYZ System* satisfies the requirements of Discretionary Access Control, Object Reuse, Identification and Authentication, System Integrity, Trusted Facility Manual, Security Test

Documentation, Security Features User's Guide, Security Network Design Documentation and Security Testing.
The evaluation concluded that the *XYZ System* partially satisfies the requirements of System Architecture and Audit. Considering that Configuration Management activities are conducted however, it is currently an informal process and that the most critical and potentially harmful user actions are audited, the identified vulnerabilities are considered to pose a Low Risk to the *XYZ System* and the data residing on it.

Determination

Based on supporting documentation, Security Testing & Evaluation results, and interviews with the XYZ System Network Administrator and Information Systems Security Officer (ISSO), adequate security controls are currently in place to justify an IATO for the *XYZ System*.

Next Steps

The *XYZ System* will provide the MHS Information Assurance (IA) Program Office the required information and documentation to complete a full Approval to Operate (ATO) in accordance with the DoD Information Technology Security Certification and Accreditation Process (DITSCAP). Accreditation activities will be completed within the negotiated timeline between the MHS IA Program Office and **XYZ System** personnel.

Appendix A
DoD Minimum C2 Security Requirements

DoD MINIMUM C2 SECURITY REQUIREMENTS - DoD 5200.28-STD

Discretionary Access Control. Restrict access to objects (e.g., files), based on the identity of individuals or defined groups of individuals, to protect objects from unauthorized access and to limit propagation of access rights.

Object Reuse. Eliminate all residual data from a medium (page frame, disk sector, and magnetic tape) before reassignment of that medium from one subject to another subject.

Identification and Authentication. Identify each individual user of the system prior to allowing user activity on that system. Establish protective mechanisms (e.g., passwords) to authenticate the user's identity and to associate this identity with all auditable actions taken by that user.

Audit. Create and maintain an audit trail so that all actions affecting the security of a system can be traced to the responsible party based on individual identity. The system must also protect the audit information from modification or unauthorized access or destruction.

System Architecture. Create and maintain a domain for execution to protect the Trusted Computing Base (TCB) from external interference or tampering, so that the TCB may protect its resources via access controls and audit trails.

System Integrity. Provide hardware/software features that will validate the correct operation of the hardware/software/firmware elements of the TCB.

Security Testing. Test security protection mechanisms to confirm that they work as claimed in the system documentation. Search for obvious flaws that would enable bypass of the security mechanisms, violation of resource isolation, and unauthorized access to the audit or authentication data.

Security Features Users Guide. Prepare a section in the user documentation describing the protection mechanisms provided by the TCB, guidelines on their use, and how they interact with one another.

Trusted Facility Manual. Prepare documentation presenting the cautions about functions and privileges needing to be controlled when running a secure facility, as well as procedures for examining and maintaining audit files. Provide a detailed audit record structure for each type of audit event.

Test Documentation. Prepare documentation that describes the test activities and results of the security mechanisms' functional testing.

Design Documentation. Make available the manufacturer's documentation that describes their philosophy of protection and how it is translated into the TCB, and if distinct TCB modules exist, the description of the interfaces between these modules.

Appendix B
MHS IA Standard Definition of Terms

MHS IA Standard Definition of Terms

Access A specific type of interaction between a subject and an object resulting in the flow of information from one to the other.

Access Control The process of limiting access to the resources of a system only to authorized programs, processes, or other systems (in a network).

Access List A list of users, programs, and/or processes and the specifications of access categories to which each is assigned.

Access Types The nature of an access right to a particular device, program, or file (e.g., read, write, execute, append, modify, delete, or create).

Accountability The property that enables activities on a system to be traced to individuals who may then be held responsible for their actions.

Accreditation A formal declaration by the DAA that the AIS and network is to operate in a particular security mode using a prescribed set of safeguards. Accreditation is the official management authorization for operation of AISs and networks on the certification process, as well as other management considerations. The accreditation statement affixes security responsibility with the DAA and shows that due care has been taken for security.

Assurance A measure of confidence that the security features and architecture of an AIS and network accurately mediate and enforce the security policy.

Audit Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established polices and operational procedures, and to recommend changes in controls, policies, or procedures.

Audit Trail A chronological record of system activities sufficient to enable the reconstruction, reviewing, and examination of the sequence of environments and activities surrounding or leading to an operation, a procedure, or an event in a transaction from its inception to final results.

Authenticate To verify the identity of a user, device, or other entity in a computer system, often as a prerequisite to allowing access to resources in a system.

Authorization The granting of access rights to a user, program, or process by a responsible administrator.

Automated Information System An assembly of computer hardware, software, and/or firmware configured to collect, create, communicate, compute, disseminate, process, store, and/or control data or information.

Automated Information System Security Measures and controls that protect an AIS and network against denial of service and unauthorized (accidental or intentional) disclosure, modification, or destruction of AISs and data. AIS and network security includes consideration of all hardware and/or software functions.

Availability Timely, reliable access to information and information services for authorized users.

Backup A copy of data and/or applications contained in the AIS/network and stored on magnetic media outside of the AIS/network to be used in the event AIS/network data are lost.

Certification The comprehensive evaluation of the technical and non-technical security features of an AIS/network and other safeguards, made in support of the accreditation process that establishes the extent to which a particular design and implementation meet a specified set of security requirements.

Communications Security A combination of technical measures designed to protect confidentiality, integrity, and availability of information while being transmitted on a telecommunications system Communications security includes crypto security, transmission security, emission security, and physical security of communication security material and information.

Compromise A violation of the security policy of a system such that unauthorized disclosure of sensitive information may have occurred.

Computer Abuse The misuse, alteration, disruption, or destruction of data processing resources. The key aspect is that it is intentional and improper.

Computer Fraud Computer-related crimes involving deliberate misrepresentation, alteration or disclosures of data in order to obtain something of value (usually for monetary gain). A computer system must have been involved in the perpetration or cover-up of the act or series of acts. A computer system might have been involved through improper manipulation of input data; output or results; applications programs; data files; computer operations; communications; or computer hardware, systems software, or firmware.

Computer Matching Program Any computerized comparison of two or more automated systems of records or a system of records with non-Federal records for the purpose of establishing or verifying the eligibility of, or continuing compliance with statutory and regulatory requirements

Confidentiality Assurance that information is not disclosed to unauthorized persons, processes, or devices.

Configuration Control The process of controlling modifications to the system's hardware, firmware, software, documentation, test, test fixtures, and test documentation that provides sufficient assurance that the system is protected against the introduction of improper modifications prior to, during, and after system implementation. See configuration management.

Configuration Management The management of security features and assurances through control of changes made to a system's hardware, software, firmware, documentation, test, test fixtures, and test documentation throughout the development and operational life of the system. See configuration control.

Contingency Plan A plan for emergency response, backup operations, and post-disaster recovery maintained by an activity as a part of its security program that will ensure the availability of critical resources and facilitate the continuity of operations in an emergency situation.

Controlled Access Protection Access control through login procedures, audit of security relevant events, and resource isolation.

Countermeasure Any action, device, procedure, technique, or other measure that reduces the vulnerability of, or threat to, a system.

Criticality Any information or applications, which are so important to the organization that little or no loss of availability is acceptable.

Cryptography The principles, means and methods for rendering information unintelligible and for restoring encrypted information to intelligible form

Data A representation of facts, concepts, information, or instructions suitable for communication, interpretation, or processing by users or by an AIS.

Data Integrity The state that exists when automated data is the same as that in source documents, or has been correctly computed from source data, and has not been exposed to alteration or destruction.

Defense-in-Depth The security approach whereby layers of IA solutions are used to establish an adequate IA posture. Implementation of this strategy also recognizes that due to the highly interactive nature of the various systems and networks, IA solutions must be considered within the context of the shared risk environment and that any single system cannot be adequately secured unless all interconnected systems are adequately secured.

Degauss To demagnetize a tape or other magnetic storage media leaving little or no magnetically stored information.

Denial of Service Any action or series of actions that prevent any part of a system from functioning in accordance with its intended purpose. This includes any action that causes unauthorized destruction, modification, or delay of service.

Designated Approving Authority (DAA) The official who has the authority to decide on accepting the security safeguards prescribed for an AIS and network or that official who may be responsible for issuing an accreditation statement that records the decision to accept those safeguards.

Disaster Recovery Plan A plan for emergency response, backup operations, and post-disaster recovery to ensure the availability of critical resources and continuity of operations in an emergency.

Discretionary Access Control A means of restricting access to objects based on the identity and need-to-know of the user, process and/or groups to which they belong. The controls are discretionary in the sense that a subject with certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject.

DoD Trusted Computer System Evaluation Criteria A document published by the National Computer Security Center containing a uniform set of basic requirements and evaluation classes for assessing degrees of assurance in the effectiveness of hardware and software security controls built into systems. These criteria are intended for use in the design and evaluation of systems that will process and/or store sensitive or classified data. This document is Government Standard DoD 5200.28-STD and is frequently referred to as "The Criteria" or "The Orange Book."

Encryption A procedure to convert plain text into cipher text.

Formal Access Approval Documented approval by a data owner to allow access to a particular category of information.

Functional Testing The segment of security testing in which the advertised security mechanisms of the system are tested, under operational conditions, for correct operation.

Identification The process that enables recognition of an entity by a system, generally by the use of unique machine-readable user names.

Information Assurance Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation.

Information System Security Officer The person responsible for ensuring that security is provided for, and implemented throughout, the life cycle of an AIS/network from the beginning of the concept development plan through its design, development, operation, maintenance, and secure disposal.

Information Assurance Vulnerability Alert Comprehensive distribution process for notification of CINCs, Services, and Agencies about vulnerability alerts and countermeasures information.

Interim Approval to Operate Temporary approval granted by a DAA for an AIS to process information based on preliminary results of a security evaluation of the system.

Isolation The containment of subjects and objects in a system in such a way that they are separated from one another, as well as from the protection controls of the operating system.

Least privilege The principle that requires each subject be granted the most restrictive set of privileges needed for the performance of authorized tasks. The application of this principle limits the damage that can result from accident, error, or unauthorized use.

Mission Critical Systems handling information, which is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness.

National Computer Security Center Originally named the DoD Computer Security Center, the NCSC is responsible for encouraging the widespread availability of trusted computer systems throughout the Federal Government.

Need-to-Know The necessity for access to, knowledge of, or possession of specific information required to carry out official duties.

Network A network is composed of a communications medium and all components attached to that medium whose responsibility is the transference of information.

Non-repudiation The method by which the sender of information is provided with proof of delivery and the recipient is assured of the sender's identity so that neither can later deny having processed the information.

Object A passive entity that contains or receives information. Access to an object potentially implies access to the information it contains. Examples of objects are: records, blocks, pages, segments, files, directories, directory trees, and programs, as well as bits, bytes, words, fields, processors, video displays, keyboards, clocks, printers, and network nodes.

Object Reuse The reassignment and reuse of a storage medium (e.g., page frame, disk sector, and magnetic tape) that once contained one or more objects. To be securely reused and assigned to a new subject, storage media must contain no residual data (magnetic remnants) from the object(s) previously contained in the media.

Operational Testing The segment of security testing in which the advertised security mechanisms of the system are tested, under operational conditions, for correct operation.

Password A protected, private character string used to authenticate an identity.

Permissions A description of the type of authorized interactions a subject can have with an object. Examples include read, write, execute, add, modify, and delete.

Personal Digital Assistant A PDA is a hand-held computer that helps with such tasks as taking notes, scheduling appointments, and sending faxes and electronic mail. PDAs are also called Personal Communicators and Personal Intelligent Communicators.

Personal Information Information about an individual that is intimate or private to the individual, as distinguished from information related solely to the individual's official functions or public life.

Personnel Security The procedures established to ensure that all personnel who have access to sensitive information have the required authority, as well as appropriate clearances.

Physical Security The application of physical barriers and control procedures as preventive measures or countermeasures against threats to resources and sensitive information.

Program Manager The person ultimately responsible for the overall procurement, development, integration, modification, or operation and maintenance of the AIS.

Privileges A set of authorization/permissions granted by an authorized officer to an AIS and network or network user to perform certain operations.

Public Key Infrastructure An enterprise-wide service that supports digital signatures and other public key-based security mechanisms for DoD functional domain programs, including generation, production, distribution, control, and accounting of public key certificates.

Reliability The quality of producing the same results each time the same procedures and products are used, usually implying dependable equipment and bug-free processing routines.

Residual Risks The portion of risk that remains after security measures have been applied.

Risk The probability that a particular threat will exploit a particular vulnerability of the system.

Risk Analysis The process of identifying security risks, determining their magnitude, and identifying areas needing safeguards. Risk analysis is a part of risk management.

Risk Assessment An assessment of a system based on the sensitivity of information processed, or to be processed, and the clearances of users to determine the Security Class of the system.

Risk Management The total process of identifying, controlling, and eliminating or minimizing uncertain events that may affect system resources. It includes risk analysis, cost benefit analysis, selection, implementation and testing, security evaluation of safeguards, and overall security review.

Safeguards An implementation of technology or techniques to protect confidentiality, integrity, and availability.

Security Evaluation An evaluation done to assess the degree of trust that can be placed in systems for the secure handling of sensitive information. One type, a product evaluation, is an evaluation performed on the hardware and software features and assurances of a computer product from a perspective that excludes the application environment. The other type, a system evaluation, is done to access a system's security safeguards with respect to a specific operational mission and is a major step in the certification and accreditation process.

Security Features The security-relevant functions, mechanisms, and characteristics of system hardware and software. Security features are a subset of system security safeguards.

Security Measures Elements of software, firmware, hardware, or procedures included in a system for the satisfaction of security specifications.

Security Policy The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information.

Security Requirements The types and levels of protection necessary for equipment, data, information, applications, personnel and facilities to meet security policy.

Security Requirements Baseline A description of minimum requirements necessary for a system to maintain an acceptable level of security.

Security Safeguards The protective measures and controls prescribed to meet the security requirements specified for a system. Those safeguards may include, but are not necessarily limited to: hardware and software security features, operating procedures, accountability procedures, access and distribution controls, management constraints, personnel security, and physical structures, areas, and devices.

Security Specifications A detailed description of the safeguards required to protect a system.

Security Test and Evaluation An examination and analysis of the security safeguards of a system as they have been applied in an operational environment to determine the security posture of the system.

Sensitive But Unclassified Information which could adversely affect national security or other Federal Government interests if it were disclosed, lost, misused, altered, or destroyed.

Sensitive Information Any information, the loss, misuse, modification of, or unauthorized access to, could adversely affect the national interest or the conduct of Federal programs. Also, information to which individuals are entitled privacy under Section 552a of Title 5, U.S. Code, (The Privacy Act) but has not been specifically authorized under criteria established by an Executive order or an act of Congress to be kept classified.

System Availability The state that exists when required automated information services can be performed within an acceptable time even under adverse circumstances.

System Integrity The quality that a system has when it performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

Technical Vulnerability A hardware, firmware, communication, or software flaw that leaves a computer processing system open for potential exploitation, either externally or internally, thereby resulting in risk for the owner, user, or manager of the system.

Terminal Identification The means used to uniquely identify a terminal to a system.

Threat Any circumstance or event with the potential to cause harm to a system in the form of destruction, disclosure, modification of data, and/or denial of service.

Threat Agent A method used to exploit a vulnerability in a system, operation, or facility.

Threat Analysis The examination of all actions and events that might adversely affect a system or operation.

Threat Monitoring The analysis, assessment, and review of audit trails and other data collected for the purpose of searching out system events that may constitute violations or attempted violations of system security.

Trusted Computer System A system that employs sufficient hardware and software assurance measures to allow its use for simultaneous processing of a range of sensitive or classified information.

Trusted Computing Base The totality of protection mechanisms within a computer system, including hardware, firmware, and software, the combination of which is responsible for enforcing a security policy. A TCB consists of one or more components that together enforce a unified security policy over a product or system. The ability of a TCB to enforce correctly a unified security policy depends solely on the mechanisms within the TCB and on the correct input by system administrative personnel of parameters (e.g., a user's clearance level) related to the security policy.

User Person or process accessing an AIS or network either by direct connections (i.e., via terminals), or indirect connections (i.e., prepare input data or receive output not reviewed for content or classification by a responsible individual).

UserID A unique symbol or character string used by a system to identify a specific user.

Virus A self-propagating computer program composed of a mission component, a trigger component, and a self-propagating component.

Vulnerability A weakness in system security procedures, system design, implementation, internal controls, etc., that could be exploited to violate system security policy.

Vulnerability Analysis The systematic examination of systems in order to determine the adequacy of security measures, identify security deficiencies, and provide data from which to predict the effectiveness of proposed security measures.

Appendix C
XYZ System Test Plan

Military Health System (XYZ System) Test Plan

Generic Test Plan is being developed and will be incorporated into this template. In the interim – this is the plan being used.

Introduction

A Risk Assessment for the System Full Name (*XYZ System*) was performed to ascertain the extent to which it meets the Department of Defense (DoD) C2 security requirements in order to obtain an Interim Approval to Operate (IATO).

The *XYZ System* testing was conducted at 111 Market Place, Baltimore, Maryland on December 19, 2001.

The *XYZ System* System Administrator and Information Systems Security Officer, and a member of the MHS Information Assurance Team conducted the tests.

Limitations

The risk assessment is a preliminary evaluation of the *XYZ System* to uncover potential threats, vulnerabilities, and points of failure that can affect the confidentiality, integrity, and availability of the network. The activity considers major factors in risk management, the value of the system or application, threat, vulnerabilities, and the effectiveness of the proposed safeguards. This risk assessment is an interim measure within the MHS full certification and accreditation process to ascertain the security threats and vulnerabilities of the *XYZ System* in advance of a full Approval to Operate (ATO) in order to achieve key project milestones or continued sustainment.

Assumptions

The following assumptions were made during this risk assessment:

3. If the network does not meet the requirements stated in the System Security Authorization Agreement (SSAA), but mission criticality mandates that the system become/remain operational, an IATO may be issued at the direction of the DAA. The MHS DAA, MHS CA, and user representative will determine the proposed solutions, schedule, security actions, milestones, and maximum length of time for the IATO validity.
4. The *XYZ System* personnel will address all the security parameters identified in the SSAA and resolve security deficiencies identified in this report within the time period identified to achieve an ATO.
5. The *XYZ System* personnel will comply with all applicable established DoD security policies, standards and guidelines throughout the network development lifecycle.
6. The *XYZ System* personnel will perform mandatory security training for the Information System Security Officer, network and system administrators, and users as identified in the system security training plans.
7. The *XYZ System* will operate in a secured environment in accordance with site operational and environmental procedures to ensure that risk to confidentiality, integrity, availability, and accountability of the information and network remains acceptable.

Testing Approach

This risk assessment was limited to the *XYZ System* directly supporting the MHS TRICARE mission. Testing and analysis was limited to the basic configuration of the *XYZ System* Windows NT 4.0 servers that process TRICARE Medical Activity (TMA) data and the extent to which the security mechanisms satisfy the minimum DoD C2 requirements listed in Appendix A.

A review of applicable documentation as described in section 3.2 of the Risk Assessment was conducted in addition to minimum ST&E activities as detailed in Appendix D.

Automated vulnerability scanning tools were not utilized at this time but will be utilized in Phase III of the full certification and accreditation process.

A total of 10 *XYZ System* servers were identified as processing TRICARE Medical Activity data. A sampling of 5 XYZ System servers were tested in support of an IATO. The configuration of all 10 servers is reportedly consistent. No variances in the configurations were found among the 5 servers that were tested. The following servers were tested:

8. XYZ System_SVR_01 (domain controller)
9. XYZ System_SVR_02 (domain controller)
10. XYZ System_SQL_01 (sql databases)
11. XYZ System_ATC_PROD1 (application server)
12. XYZ System_EXCHG (mail server)

Appendix D
XYZ System Test Procedures and Results

XYZ System Test Procedures and Results

Generic Test Plan is being developed and will be incorporated into this template

TEST OBJECTIVE	Test Procedure	Expected Results	Results (Pass, Fail, or Partially Satisfied)
Test Set: Access			
Test #1			